PACiS SYSTEM

PACiS/EN TG/C80

System Guide

Schneider Electric

PACiS SYSTEM
CONTENT

Safety & Handling	**PACiS/EN SA/C80**
Introduction	**PACiS/EN IT/C80**
Installation	**PACiS/EN IN/C80**
Functional Description	**PACiS/EN FT/C80**
Lexical	**PACiS/EN LX/C80**
Cyber Security	**PACiS/EN CS/C80**

BLANK PAGE

SAFETY & HANDLING

CONTENTS

1.	**INTRODUCTION**	**3**
2.	**SAFETY**	**4**
2.1	**Health and Safety**	**4**
2.2	**Explanation of symbols and labels**	**4**
2.3	**Installing, Commissioning and Servicing**	**4**
2.4	**Decommissioning and Disposal**	**4**
3.	**GUARANTIES**	**5**
4.	**COPYRIGHTS & TRADEMARKS**	**6**
4.1	**Copyrights**	**6**
4.2	**Trademarks**	**6**
5.	**WARNINGS REGARDING USE OF SCHNEIDER ELECTRIC PRODUCTS**	**7**

BLANK PAGE

1. INTRODUCTION

The present document is a chapter of PACiS SYSTEM documentation binders. It describes the safety, handling, packing and unpacking procedures applicable to PACiS SYSTEM elements.

2. SAFETY

WARNING: THIS SAFETY SECTION SHOULD BE READ BEFORE COMMENCING ANY WORK ON THE EQUIPMENT.

2.1 Health and Safety

The information in the Safety Section of the PACiS System documentation is intended to ensure that products are properly installed and handled in order to maintain them in a safe condition. It is assumed that everyone who will be associated with the PACiS System equipments will be familiar with the contents of the different PACiS System Safety Sections and all Safety documents related to the PC and Communication networks.

2.2 Explanation of symbols and labels

The meaning of symbols and labels may be used on the PACiS System equipments or in the PACiS System product documentation, is given below.

2.3 Installing, Commissioning and Servicing

Equipment operating conditions

The PACiS System equipments should be operated within the specified electrical and environmental limits.

Fibre optic communication

Optical LED transceivers used in Switch boards are classified as IEC 825-1 Accessible Emission Limit (AEL) Class 1 and consequently considered eye safe.

Optical power meters should be used to determine the operation or signal level of the device.

2.4 Decommissioning and Disposal

Disposal:

It is recommended to avoid incineration and disposal of the PACiS System elements (hardware and software supports). The PACiS System elements should be disposed of in a safe manner.

3. GUARANTIES

The media on which you received Schneider Electric software are guaranteed not to fail executing programming instructions, due to defects in materials and workmanship, for a period of 90 days from date of shipment, as evidenced by receipts or other documentation. Schneider Electric will, at its option, repair or replace software media that do not execute programming instructions if Schneider Electric receives notice of such defects during the guaranty period. Schneider Electric does not guaranty that the operation of the software shall be uninterrupted or error free.

A Return Material Authorisation (RMA) number must be obtained from the factory and clearly marked on the package before any equipment acceptance for guaranty work. Schneider Electric will pay the shipping costs of returning to the owner parts, which are covered by warranty.

Schneider Electric believes that the information in this document is accurate. The document has been carefully reviewed for technical accuracy. In the event that technical or typographical errors exist, Schneider Electric reserves the right to make changes to subsequent editions of this document without prior notice to holders of this edition. The reader should consult Schneider Electric if errors are suspected. In no event shall Schneider Electric be liable for any damages arising out of or related to this document or the information contained in it.

Expect as specified herein, Schneider Electric makes no guaranties, express or implied and specifically disclaims and guaranties of merchantability or fitness for a particular purpose.

Customer's rights to recover damages caused by fault or negligence on the part Schneider Electric shall be limited to the amount therefore paid by the customer. Schneider Electric will not be liable for damages resulting from loss of data, profits, use of products or incidental or consequential damages even if advised of the possibility thereof.

This limitation of the liability of Schneider Electric will apply regardless of the form of action, whether in contract or tort, including negligence. Any action against Schneider Electric must be brought within one year after the cause of action accrues. Schneider Electric shall not be liable for any delay in performance due to causes beyond its reasonable control.

The warranty provided herein dues net cover damages, defects, malfunctions, or service failures caused by owner's failure to follow the Schneider Electric installation, operation, or maintenance instructions; owner's modification of the product; owner's abuse, misuse, or negligent acts; and power failure or surges, fire, flood, accident, actions of third parties, or other events outside reasonable control.

4. COPYRIGHTS & TRADEMARKS

4.1 Copyrights

Under the copyright laws, this publication may not be reproduced or transmitted in any form, electronic or mechanical, including photocopying, recording, storing in an information retrieval system, or translating, in whole or in part, without the prior written consent of Schneider Electric.

4.2 Trademarks

PACiS, PACiS SCE, PACiS ES, PACiS SMT, PACiS OI, PACiS MiCOM are trademarks of Schneider Electric.

Product and company names mentioned herein are trademarks or trade names of their respective companies.

5. WARNINGS REGARDING USE OF SCHNEIDER ELECTRIC PRODUCTS

Schneider Electric products are not designed with components and testing for a level of reliability suitable for use in or in connection with surgical implants or as critical components in any life support systems whose failure to perform can reasonably be expected to cause significant injuries to a human.

In any application, including the above reliability of operation of the software products can be impaired by adverse factors, including -but not limited- to fluctuations in electrical power supply, MiCOM C264 hardware malfunctions, MiCOM C264 operating system, software fitness, fitness of compilers and development software used to develop an application, installation errors, software and hardware compatibility problems, malfunctions or failures of electronic monitoring or control devices, transient failures of electronic systems (hardware and/or software), unanticipated uses or misuses, or errors from the user or applications designer (adverse factors such as these are collectively termed "System failures").

Any application where a system failure would create a risk of harm to property or persons (including the risk of bodily injuries and death) should not be reliant solely upon one form of electronic system due to the risk of system failure to avoid damage, injury or death, the user or application designer must take reasonably steps to protect against system failure, including -but not limited- to back-up or shut-down mechanisms, not because end-user system is customised and differs from Schneider Electric testing platforms but also a user or application designer may use Schneider Electric products in combination with other products.

These actions cannot be evaluated or contemplated by Schneider Electric; Thus, the user or application designer is ultimately responsible for verifying and validating the suitability of Schneider Electric products whenever they are incorporated in a system or application, even without limitation of the appropriate design, process and safety levels of such system or application.

BLANK PAGE

INTRODUCTION

CONTENTS

1. INTRODUCTION 3

1.1 Scope of the document 3

1.2 Introduction to PACiS 3

2. DOCUMENTATION 5

2.1 Chapter descriptions 5

2.1.1 Safety and Handling (SA) Chapter 5

2.1.2 Introduction (IT) Chapter 5

2.1.3 Functional Description (FT) Chapter 5

2.1.4 Installation (IN) Chapter 5

2.1.5 Lexicon (LX) Chapter 5

BLANK PAGE

1. INTRODUCTION

1.1 Scope of the document

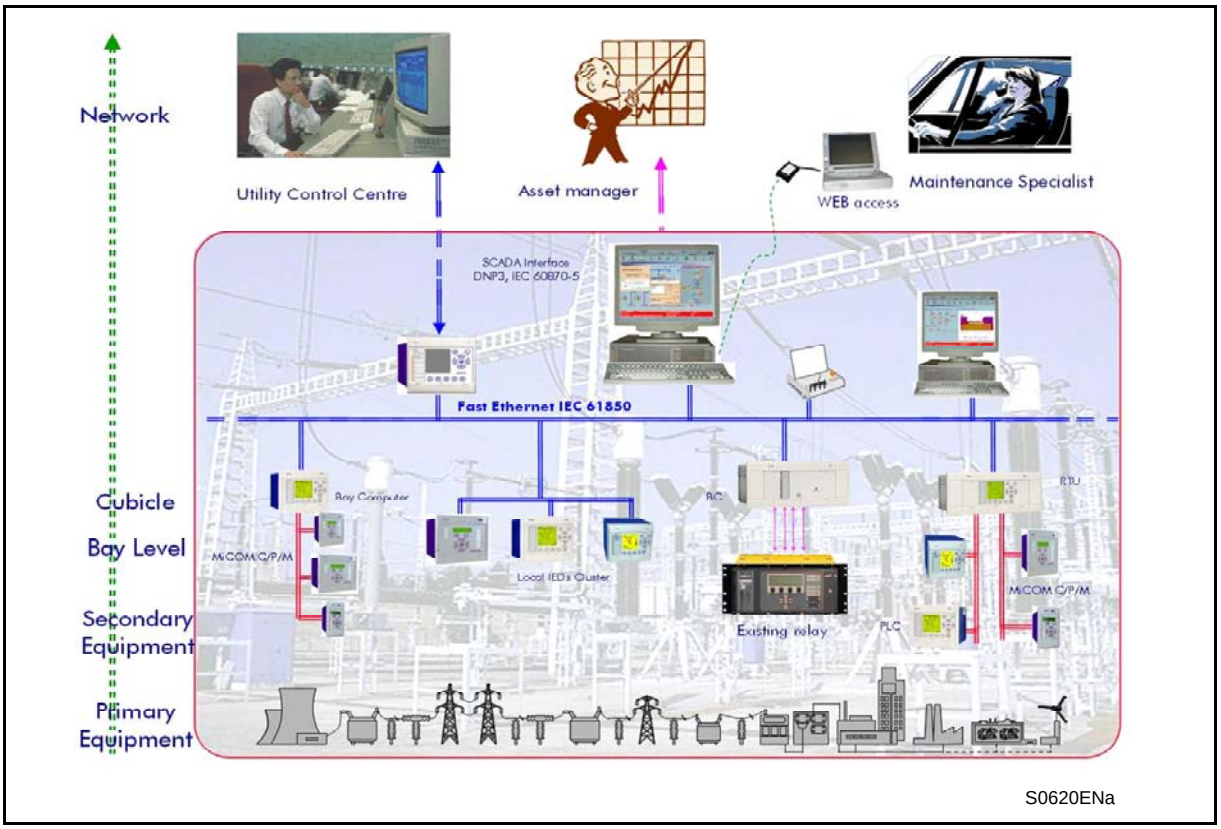
This version of the PACiS documentation refers to version PACiS V4.8. This document is a chapter of PACiS System documentation binders. It introduces the user to the PACiS system and its elements documentation.

1.2 Introduction to PACiS

PACiS offers a flexible answer to electrical substation Protection, Automation, Control and Monitoring requirements. PACiS is designed for new and retrofit application cases with dedicated features enabling an easy system extension and a minimization of outage time during retrofit.

PACiS is based on a unique configurable architecture, in term of functions, performances and physical distribution within one or several substations.

The PACiS System architecture is always based on a Station Bus IEC61850 to which is connected equipment used for the customer solution.



This equipment includes:

- the Operator Workstation(s) (Local HMI of the site) PACiS OI
- the Computers MiCOM C264, or C264P with feeder protection
- the SCADA gateway PACiS GTW based on the MiCOM A300 PC
- the Ethernet switches MiCOM H

The Station Bus is based on the IEC61850 protocol, over an Ethernet / TCP-IP network. Additional busses (called legacy buses) are also available in the PACiS System architectures.

The typical PACiS architecture based on MiCOM elements ensures:

- maximise the functional integration through fast exchanges between devices (10/100 Mbps)
- allow a flexible distribution inside or between substations
- integrate third party devices within the Digital Control System of the substation

PACiS offers connection with legacy communication networks (RS232, RS485, optical) in order to fully re-used past investments with the new generation.

2. DOCUMENTATION

The guides provide a functional and technical description of the PACiS elements and a comprehensive set of instructions for the PACiS elements's use and application.

A System Guide is provided at system level: it contains chapters listed and described below. More detailed guides (Operation Guide, Technical Guide, Getting Started Guide) are provided at equipment level.

Due to the specific construction and application of each PACiS element, the content of each PACiS element is adapted and some chapters do not exist in the relevant documents

2.1 Chapter descriptions

2.1.1 Safety and Handling (SA) Chapter

This chapter contains the safety instructions, handling and reception of electronic equipment, packing and unpacking parts, Copyrights and Trademarks.

2.1.2 Introduction (IT) Chapter

This document contains the description of each document, and an outline of the product features.

2.1.3 Functional Description (FT) Chapter

This chapter contains a description of function supported by the product.

2.1.4 Installation (IN) Chapter

This chapter contains the installation procedures.

2.1.5 Lexical (LX) Chapter

This chapter contains lexical description of acronyms and definitions.

BLANK PAGE

INSTALLATION

CONTENTS

1.	**INTRODUCTION**	**3**
1.1	**Scope of the document**	**3**
2.	**SYSTEM INSTALLATION**	**4**
2.1	**Installation ordering**	**5**
2.2	**Kind of PACiS system Installation**	**5**
3.	**REQUIREMENTS**	**6**
3.1	**General PACiS system requirement**	**6**
3.2	**Basic requirement**	**6**
3.3	**Installation end requirement**	**7**
3.4	**System Commissioning Application requirement**	**7**
4.	**PACiS DEVICES INSTALLATION**	**8**
4.1	**PACiS SCE installation**	**8**
4.2	**PACiS Station Bus Agency installation**	**8**
4.3	**PACiS SMT installation**	**9**
4.4	**PACiS OI installation**	**10**
4.5	**PACiS Gateway installation**	**10**
4.6	**MiCOM C264 installation**	**11**
4.7	**PACiS Watch installation**	**11**
5.	**PACiS DEVICES INSTALLATION AS A SERVICE**	**12**
5.1	**Overview**	**12**
5.2	**Application on Windows 2003 server in service mode**	**13**
5.2.1	Installation	13
5.2.2	WinPcap settings	13
5.2.3	DCOM settings	14
5.3	**Application on Windows XP in service mode**	**17**
5.3.1	Installation	17
5.3.2	Settings	17
5.4	**Launch the application**	**18**
5.5	**PACiS Watch in service mode**	**19**
5.5.1	Setttings	20
5.5.2	Settings as a service	21
6.	**NETWORKS INSTALLATION**	**24**
6.1	**Legacy Bus installation**	**24**
6.2	**Station Bus installation**	**24**
6.3	**Telecontrol Bus installation**	**24**

7. NON PACiS DEVICES INSTALLATION 25

7.1 PACiS OI printer 25

7.2 MiCOM C264 printer 25

7.3 PACiS System Master clock 25

8. NON PACiS APPLICATIONS INSTALLATION 26

8.1 ALERT Software 26

8.1.1 Identification of the PACiS alarms to be notified 26

8.1.2 Connection between ALERT and PACiS alarms 27

8.1.3 ALERT configuration for SMS 28

8.2 Setting up a remote terminal (Windows Terminal Service) 33

8.2.1 Architectures 33

8.2.2 WTS Server installation (Windows Server 2003) 33

8.2.3 Terminal Server services configuration (Windows Server 2003) 34

8.2.4 Users statement in Active Directory 36

8.2.5 Connection to the Domain Controller in Administrator mode 38

1. INTRODUCTION

1.1 Scope of the document

This document is a chapter of the PACiS System documentation. It describes the global system installation with reference to each IN (installation) chapter of the system devices. These references are described in the chapter PACiS System IT (Introduction). Reference of non PACiS equipment is made here, with their specific and proprietary documentation.

2. SYSTEM INSTALLATION

A system installation is defined since at least two of system devices should work together. As they work together, a third component needs to be checked with the system network.

The system installation is then composed of several of the following installation:

- **1- Maintenance PC** (laptop) that might include:
  - ⇒ PACiS SCE (System Configuration Editor) to build/modify data bases,
  - ⇒ PACiS IEC-61850 Agency for communication on the SBUS,
  - ⇒ PACiS SMT (System Management Tool) to download database and manage the system
  - ⇒ PACiS CMT (Computer Management Tool) to manage the C264 computer range
  - ⇒ PACiS Documentation, system version release note and PACiS software components.
  - ⇒ Non PACiS Tools (ISaGRAF Workbench, terminal console, Serial communication spies like ASE SCADA simulator, XML Spy, FTP server…)
- **2a- MiCOM C264** installation that may include:
  - ⇒ connected IED on Legacy BUS,
  - ⇒ Computer RTU communication to SCADA (Telecontrol BUS),
  - ⇒ wiring and cubicles.
- **2b-Operator Workstation** based on industrial PC that may include:
  - ⇒ needed peripherals (printers, modem)
  - ⇒ PACiS IEC-61850 Agency for communication on the SBUS,
  - ⇒ PACiS Operator Interface
  - ⇒ PACiS System Management Tool
  - ⇒ Third-party applications
  - ⇒ PACiS Watch, to supervise at least the OI and SMT applications
- **2c-PACiS Gateway** device on industrial PC
  - ⇒ PACiS IEC-61850 Agency for communication on the SBUS,
  - ⇒ PACiS Gateways Applications for protocol communication on TBUS,
- **3a-Station BUS network** based on Ethernet network optical/copper, switch, repeater…

2.1 Installation ordering

System installation ordering follows usually the number indicated. Maintenance PC is needed at any step even network installation to check via “ping” the correct wiring.

Operator workstation, gateway and computer with their cubicle are installation tasks that can be lead in parallel.

2.2 Kind of PACiS system Installation

Installation is a step between engineering studies and commissioning. The main goal of installation is to do it in an electric plant. Further, the word “Application” is reserved for this target.

Into the standard system manufacturing process, three levels of installation are done:

- **Experimental set-up**, that uses a reduced set of devices, with the aim to validate special features and/or configuration of a set of PACiS devices; missing system devices are replaced by PACiS ES for example. Set-up is used to validate SCADA mapping and communication, SOE or alarm labels, automation, communication to IED…
- **Factory set-up** that integrates usually all system devices, not necessary mounted into cubicles, and uses **some of** system external devices like IED, or simulates them like SCADA or switch-gears. Aim is to validate customer Application needs into a FAT (Schneider Electric/VAR Factory Acceptance Test) before final delivery.
- **Site installation** is the final Application installation with all defined system interfaces fully wired and operational. The SAT (Site Acceptance Tests) ends fully this installation.

Requirements, constraints, and commissioning tests are different for each installation, and specific for final site installation power-up. The devices and configuration is specific to a given business and associate manual are defined in DCS business.

This chapter defines minimal requirements for installation procedure without particular implementation. The CM (Commissioning) chapter of each device defines how to check that PACiS device are operational and correctly installed.

Tests lead to check that system behaves correctly for a given application (with specific functions) are part of the business plan and out of scope of standard PACiS documentation. Customer found FAT and SAT validation test into their specific business plan.

3. REQUIREMENTS

System is complex. Even if its manufacturing can been done by steps, several requirements are needed before.

3.1 General PACiS system requirement

Before any installation, a versioned plan or array is needed where are defined the network parameters. It is an output of business and technical staff.

- **SBUS devices list** to install or to simulate, with:
  - ⇒ **Naming**, correct alias name on Ethernet **is mandatory**
  - ⇒ **IP address is mandatory** on Ethernet, address of IED on Legacy BUS is mandatory
  - ⇒ Hardware version and its hardware configuration (boards, voltage)
  - ⇒ Software and database version can be useful but subject to modification during commissioning
- Networks scheme is mandatory with:
  - ⇒ Networks topology drawing (ring, star) with devices reference, length between connections, additional switch, repeater
  - ⇒ Physical link to use (RS232, RS422, RS485, 10T, 100T, 100F)
  - ⇒ Protocol (IEC61850, MODBUS SCHNEIDER ELECTRIC, IEC 60870-5-103, IEC 60870-5-101, DNP3.0, IEC 60870-5-104, OPC, CDC Type 2, .GI74, HNZ, etc....)

Network name and IP address are needed before any PACiS system device installation. The network name and IP address must be identical to those configured in the PACiS SCE database. Change remains possible as described in maintenance manuals, but is time consuming operation. If address is changed all devices communicating with this past address should be reconfigured with the new address.

Clear definition of the network avoids also changing later on the communication means (physical link, speed, additional repeater) usually integrated into any Ethernet device.

3.2 Basic requirement

Even if it is trivial in engineering, before installation several checks have to be done. The above list is also a way to control that system devices ordered match installation constraints:

- PACiS system components should be present and in their ship box,
- Non PACiS components should have been correctly installed and operational. For example an other PC than the recommended one should have the needed operating software, special peripheral like printers or modems should have appropriate drivers to the PACiS OS
- Power Supply source is available with compatible voltage, power capability, stability, power source protected, and well defined power wiring
- Location for set-up has to be compatible with human security and device utilisation (mechanical support including chairs, temperature, humidity, electromagnetic field, radiation, local emergency stop…)
- Correct and operational network connection to non PACiS equipment (LBUS or SBUS link to non PACiS IED, TBUS link like PSTN to SCADA …)
- Normalised and operational wiring to electric devices (scheme, wiring, cable, shield, earthing…)
- Qualified personnel
- Certified test material and tools

3.3 Installation end requirement

Any installation process ends with a commissioning part to verify that devices operate.

PACiS devices are operational with databases. Also it is not possible to check installation in a commissioning part without downloading database into devices and check that through networks they can communicate.

Commissioning database can be an abstract of application database, or a test database with same hardware configuration and same IP address (and device name)

It is highly recommended to prepare this commissioning database before the end of installation.

3.4 System Commissioning Application requirement

Application requirement is out of scope of this document, but few requirements are here summarised.

- Process
  - ⇒ Voltage topology (with interlock…)
  - ⇒ Bay definition with additional I/O (measurements, …)
  - ⇒ Modules definition (Switch/transformer/motors..) with its I/O, control kind and delays…
  - ⇒ Protective function and devices
  - ⇒ Measurement, monitoring, metering function and devices
  - ⇒ Control functions and devices (uniqueness, mode control, AR, Synchrocheck, AVR)
  - ⇒ Non electric process (I/O GIS, security, supply control…)
- Mapping
  - ⇒ Desired information acquired from IED on Legacy BUS
  - ⇒ Desired information acquired from IED on Station BUS
  - ⇒ Desired information provided to non PACiS device on Station BUS
  - ⇒ Desired information provided to SCADA for each Tele-control BUS
- Wiring
  - ⇒ Mapping to computer connectors
  - ⇒ I/O kind AC/DC voltage or current
- Human Interface I/O
  - ⇒ MiCOM C264 configurable LED definition on computer
  - ⇒ MiCOM C264 Bay Panel definition
  - ⇒ PACiS OI and computer Alarms
  - ⇒ PACiS OI Archiving (with viewers)
  - ⇒ PACiS OI SOE and log printing (with labels)
  - ⇒ PACiS OI Mimic displays and module control
  - ⇒ PACiS OI and Computer Right definition

4. PACiS DEVICES INSTALLATION

PACiS devices installation is lead by an administrator user with:

- Hardware device (with its OS for PC applications)
- System Release notes
- Software packages
- Each device installation manual

Installation of application software on PC request administrator password.

A few devices specific recommendation are summarised below, but only each device installation manual gives the correct procedure.

4.1 PACiS SCE installation

PACiS SCE can be installed on any PC respecting its requirement.

PACiS SCE IN chapter (Installation) describes fully its requirements and install procedure. PACiS SCE MF chapter (Maintenance) describes common trouble shooting.

PACiS SCE must not run on the same PC and at the same time than PACiS OI server.

Briefly, a SCE software installation is as follows:

1. If a previous version of SCE application is installed, uninstall it
2. Launch the **SCE installer** program and follow instructions
3. If a previous version of the PACiS XML parser application is installed, uninstall it
4. Launch the **XML Parser installer** program and follow instructions

IMPORTANT:

- the "**sce.lax**" file (available in the installation folder) must be modified to update the **lax.nl.java.option.java.heap.size.max** attribute depending on the memory size of your PC (to 400 Mb if the memory size is 1Gb).
- Check the dates of the **msxml.dll** files located in **C:\WINDOWS\system32** folder: if they are different from those provided in **Tools\msxml_dlls.zip** file (on PACiS CD), replace them and do not install any third-party applications after

4.2 PACiS Station Bus Agency installation

PACiS Station Bus Agency is composed of a set of softwares to be installed on any PC supporting an Ethernet IEC61850 connection. For other devices such as MiCOM C264, Station Bus agency is part of the product and does not require any specific installation.

PACiS Station Bus IN chapter describes fully the install procedure.

Briefly, the agency software installation is as follows:

1. If a previous version of the agency is installed, uninstall it
2. Launch the **Station Bus agency installer** program and follow instructions. Three components are available:

   ⇒ the Station Bus agency,

   ⇒ the OdFoundry component, which should be installed only on the PC which supports the Equipment Simulator

   ⇒ the IED tunelling component, which should be installed if an IED setting software is used in tunelling mode

IMPORTANT:

If the PC on which the agency is installed has two Ethernet ports, a configuration file has to be modified as follows to indicate that the agency has to use the chosen port:

- open the "**lean.cfg**" file, located in the "exe" binder of the agency installation binder
- add:

```
Begin_Remote
        Common_Name     = localIP
        AP_Title        = 1 3 9999 23
        AE_Qualifier    = 1
        Psel            = 00 00 00 01
        Ssel            = 00 01
        Tsel            = 00 01
        Transport       = TCP
        NSAP            = 49 00 01 53 49 53 43 09 01 01
        Ip_addr         = <IP @>
End_Remote
```

With <IP @> the IP address of the port the agency has to connect to.

4.3 PACiS SMT installation

PACiS SMT is composed of two applications: server and client.

The station maintenance PC has licence for both applications.

SMT Server application is normally installed on main OWS that support PACiS OI server. It should be installed after PACiS OI server, even if needed to commission it.

PACiS SMT IN chapter describes fully the install procedure.

For commissioning it is reminded that client application should be only started after server application part (or kernel). When client application is remote, communication link (via ping function) should be tested before commissioning SMT client.

Briefly, a SMT software installation is as follows:

1. If a previous version of the SMT is installed, uninstall it
2. Launch the **SMT installer** program and follow instructions. Three components are available:

   ⇒ the kernel, or server: only one kernel could be installed in a PACiS system

   ⇒ the HMI, or client: one client can be installed on the PC which supports the kernel. Other clients can be installed on other PC

   ⇒ the HMI set-up, which allows to install HMI on other PC, without using the installation CD-ROM

The SMT doesn't install the Station Bus agency. If it has not been previously done, the agency must be installed.

4.4 PACiS OI installation

PACiS OI is composed of two applications: server and client.

The Operator Interface package is composed of server part (connected on SBUS) and client part displaying mimics. The PACiS OI IN chapter described fully installation requirement and procedure.

Let remind from this documentation that Microsoft Windows™ (2003 or XP) should be correctly installed before with IP and name. With remote client applications, Microsoft Windows™ 2003 SERVER should be installed first. The client commissioning suppose to check first communication to server application. Evolution from local OI client(s) to remote OI client(s) need to reinstall a Microsoft Windows™ 2003 with SERVER licence.

The Station Bus agency installation should be done before PACiS OI Server application.

Briefly, a complete (client and server) OI software installation is as follows:

1. Check if SQL Server (2000 or 2005) is installed. If no, install it. If yes, delete the "Historian" database
2. If a previous version of OI application is installed, uninstall it and reboot the PC
3. If OI and/or SCADA 2000 applications have been uninstalled, reboot the PC
4. Launch the **OI installer** and follow instructions
5. Reboot the PC

If PACiS OI and PACiS GTW are cohosted, enter both IP addresses in Internet Protocol Properties.

CAUTION

IN WINDOWS XP SP3, WHEN YOU HAVE TWO IP ADDRESSES ON THE SAME NETWORK BOARD AND A DISCONNECT FROM THE ETHERNET NETWORK OCCURS, THE PRIMARY IP ADDRESS RESETS TO 0.0.0.0. WHEN YOU RECONNECT THE ETHERNET NETWORK CABLE. WINDOWS XP SP3 DOES NOT RESTORE THE PRIMARY IP ADDRESSE.

Microsoft provides a hotfix at:

http://support.microsoft.com/kb/.896062/en-us

4.5 PACiS Gateway installation

PACiS gateway installation is described in its IN chapter.

Kind and number of SCADA communication (T-BUS) impact the hardware, and it is important to check clearly this definition before installation.

Briefly, a Gateway software installation is as follows:

1. If a previous version of gateway application is installed, uninstall it
2. Launch the **Gateway installer** and follow instructions
3. Station Bus agency is installed with the Gateway. Nevertheless, it could be necessary to install an other version of the agency, regarding the PACiS version coherency table given in each system release note.

4.6 MiCOM C264 installation

Installation is described in IN and MF (name and IP modification) chapters.

Computer is received with default IP address that need to be changed as defined into MF chapter. This installation contains additional parts on networks referenced also later in this document.

Briefly, a Computer software installation is as follows:

1. If a previous version of computer application is installed, uninstall it
2. Launch the **C264 installer** and follow instructions. Several components are available:

   ⇒ three versions of C264 computer, depending on the available hardware (CPU type). **Be careful in the choice of the version**

   ⇒ an FTP server, to allow software download in computer from the PC

   ⇒ the COMTRADE IED conversion files, if needed by third-party application. These conversion files are already installed with the SMT.

   ⇒ The PACiS CMT (Computer Maintenance Tool)

   At least one computer version, the FTP server and the CMT must be installed. The CMT will be used to set the computer for software installation.

4.7 PACiS Watch installation

PACiS Watch installation is described in the OI IN chapter.

Briefly, a PACiS Watch software installation is as follows:

1. If a previous version of PACiS Watch application is installed, **don't uninstall it**. This is recommended to keep settings of the previous version.
2. Launch the **Watch installer** and follow instructions
3. If needed, modify the PACiS Watch setting to define which applications shoould be supervised

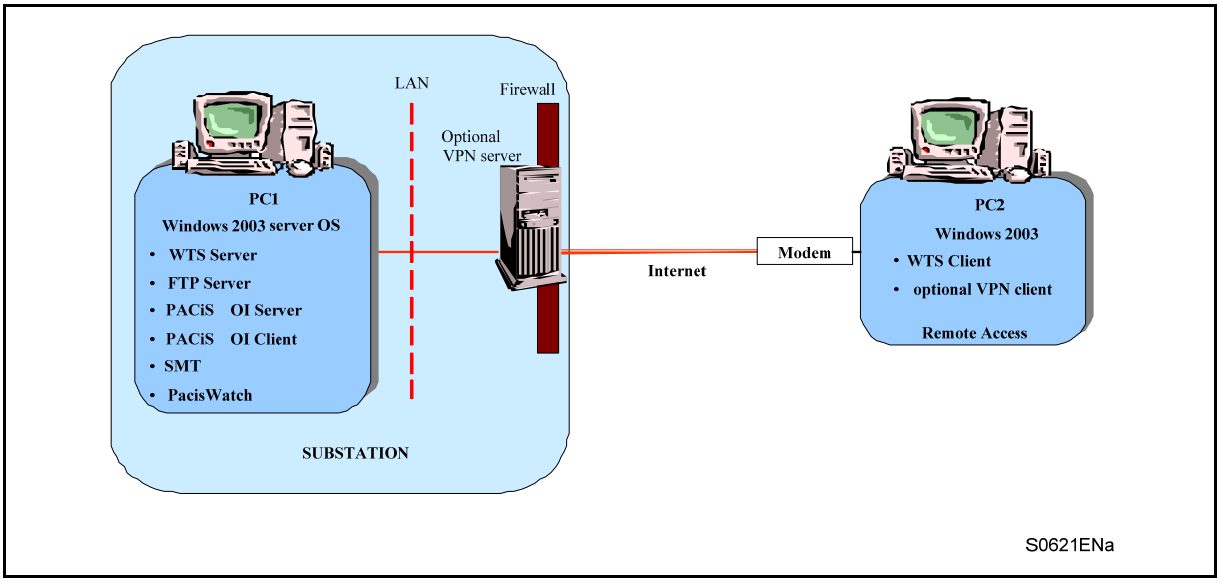
5. PACiS DEVICES INSTALLATION AS A SERVICE

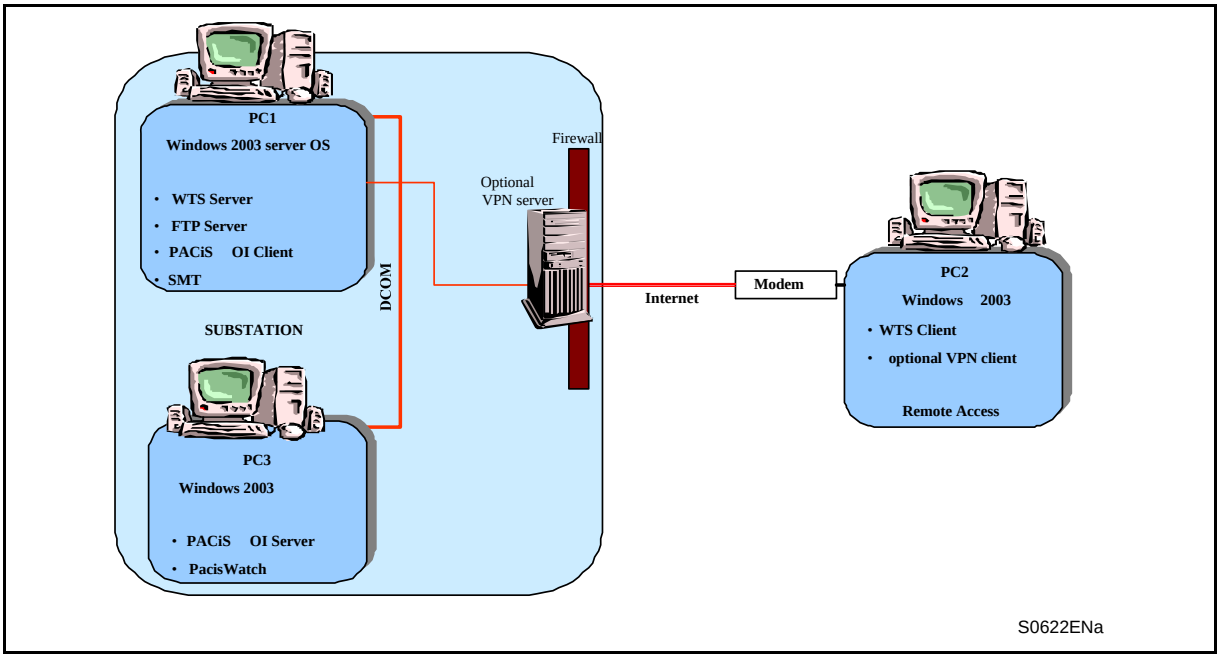
5.1 Overview

WTS (Windows Terminal Server) allows to connect to a client application remotely using the Remote Desktop Protocol over a WAN (using ADSL, modem…). To enhance security over the Internet, a VPN can be deployed; for more details refer to the appendix.

Example:

OI Server and OI Client can be installed on the same machine or not:





When the user launches a PACiS application from a WTS client PC, it will successfully communicates with the PACiS OI server, only if the latter one has been launched in a Windows service context (launched as a Windows service or launched by a Windows service). This is due to due to WTS session mechanisms.

This implies to install the server application as a service.

5.2 Application on a Windows 2003 server in service mode

For this purpose, refer to http://www.laboratoire-microsoft.org/articles/win/tse2003.

5.2.1 Installation

1. Copy InstalPacisSrv_WS2003.bat to the PACiS setup folder. The default location is C:\Program Files\USDATA\S2K\Bin
2. Copy PacisSrvkeys_WS2003.reg to PACiS setup folder. The default location is C:\Program Files\USDATA\S2K\Bin
3. Run the file InstalPacisSrv_WS2003.bat

   Note: This batch file will register S2Kserver as service and setup Register Keys.
4. Run regedit and check the value of the following key

   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\S2KServer\]

Here the entry “ImagePath” will have full path of S2KServer.exe as its value.

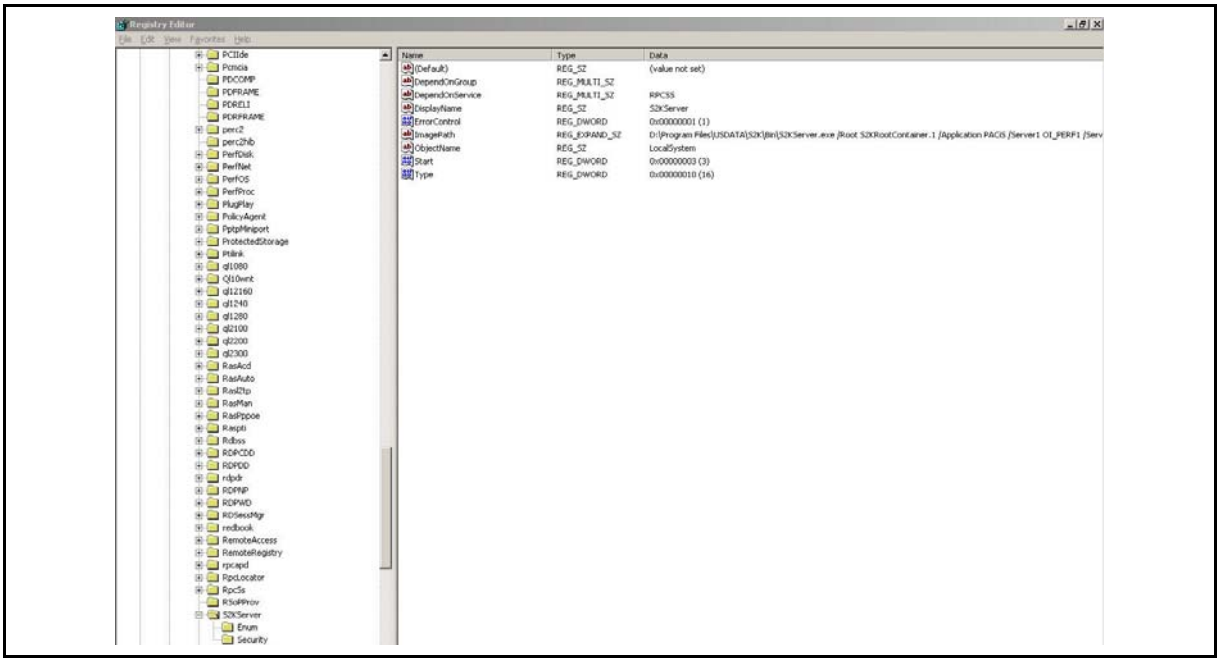
ImagePath = D:\Program Files\USDATA\S2K\Bin\S2KServer.exe

/Root S2KRootContainer.1 /Application PACiS

/Server1 OI_PERF1 /Server2 OI_PERF2 /PrsShare

PersistancePACIS /LocateTime 20000 /WaitAloneTime

20000 /StartMode WARM.



If the hot Redundancy architecture is used, InstalPacisSrv_WS2003.bat has been setup with OI Server main and Server backup (OI_PERF1 stands for the main OI server, OI_PERF2 for the back-up)

5.2.2 WinPcap settings

The use of OI Server as service with Windows Server 2003 involves the installation of WinPcap 3.0 in place of a newest version.

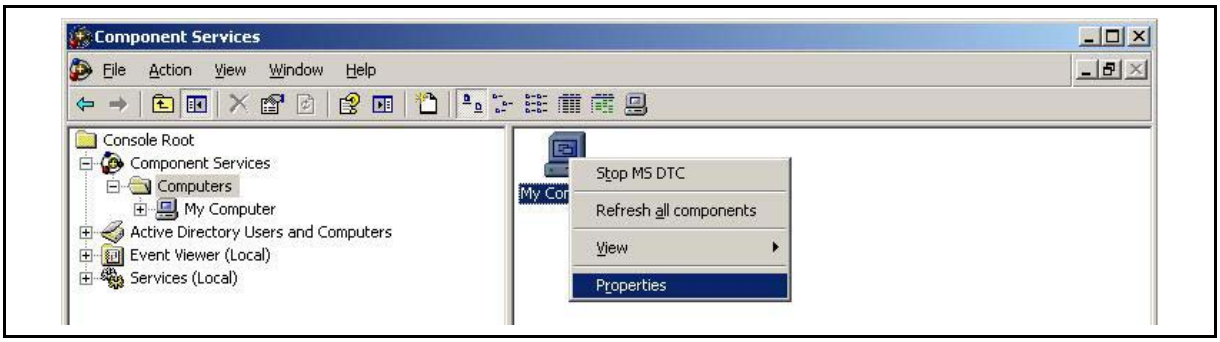
If WinPcap installed version is not the version 3.0 (e.g. 4.0.1), you have first to uninstall it from Windows.

Get the setup of WinPcap in version 3.0 from http://www.winpcap.org/archive/

5.2.3 DCOM settings

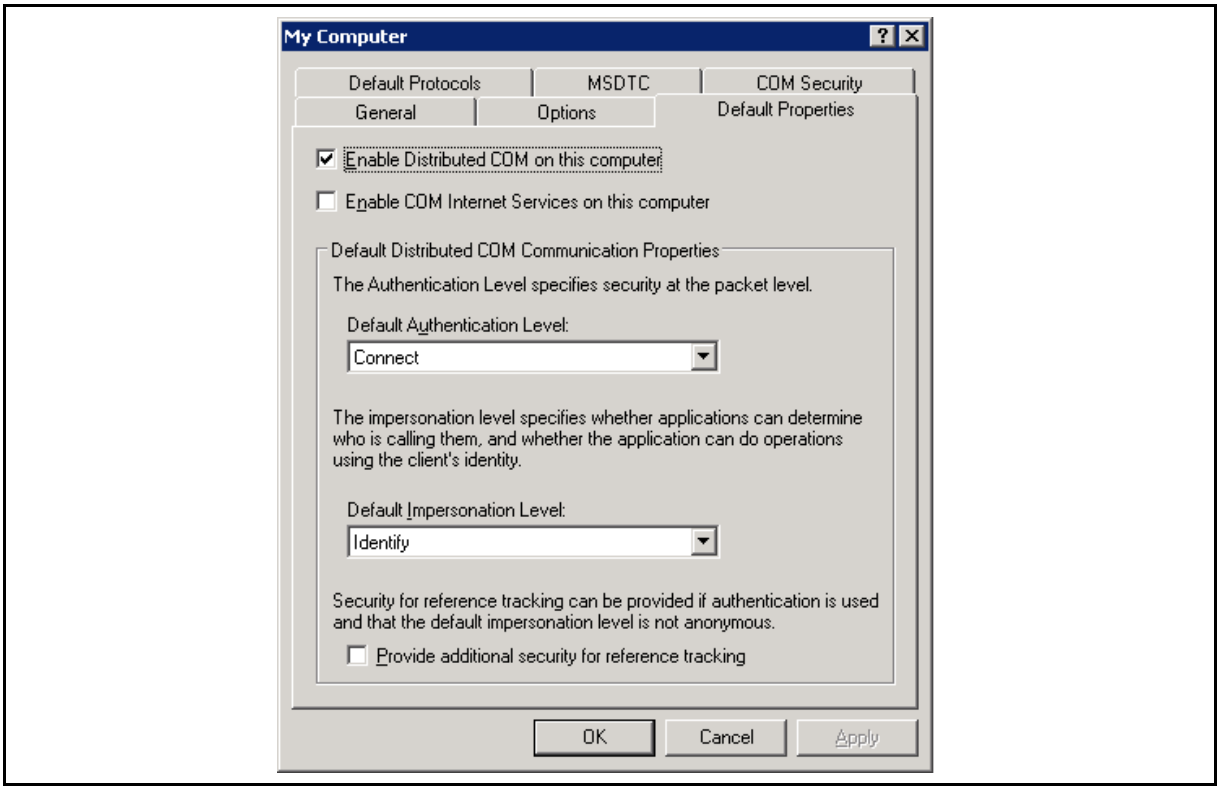
1. Copy InstalPacisSrv_WS2003.bat to the Pacis setup folder. The default location is C:\Program Files\USDATA\S2K\Bin

2. Open the “Component Services” window from Control Panel /Administrative Tools or running dcomcnfg.

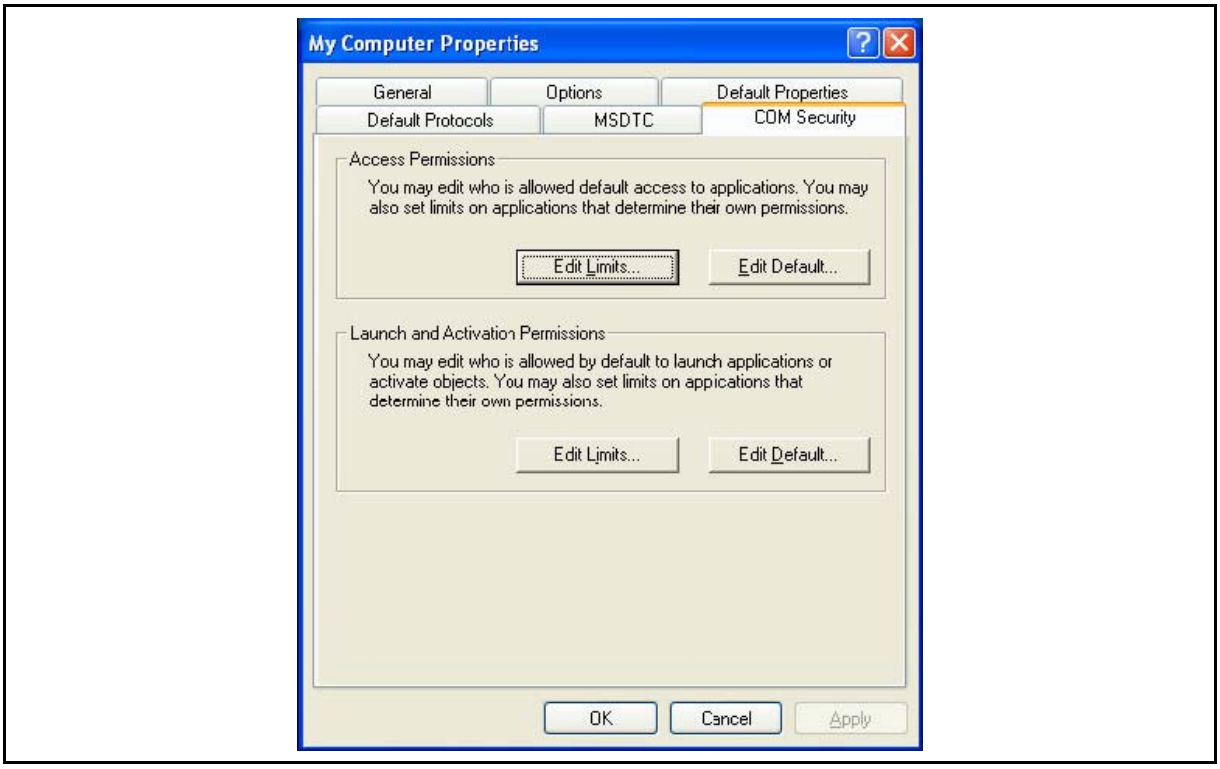


3. Click on the icon in the toolbar. Select the “Default Properties” tab of the displayed dialog. Verify that the following default properties are checked and selected. (This should be like this by default)

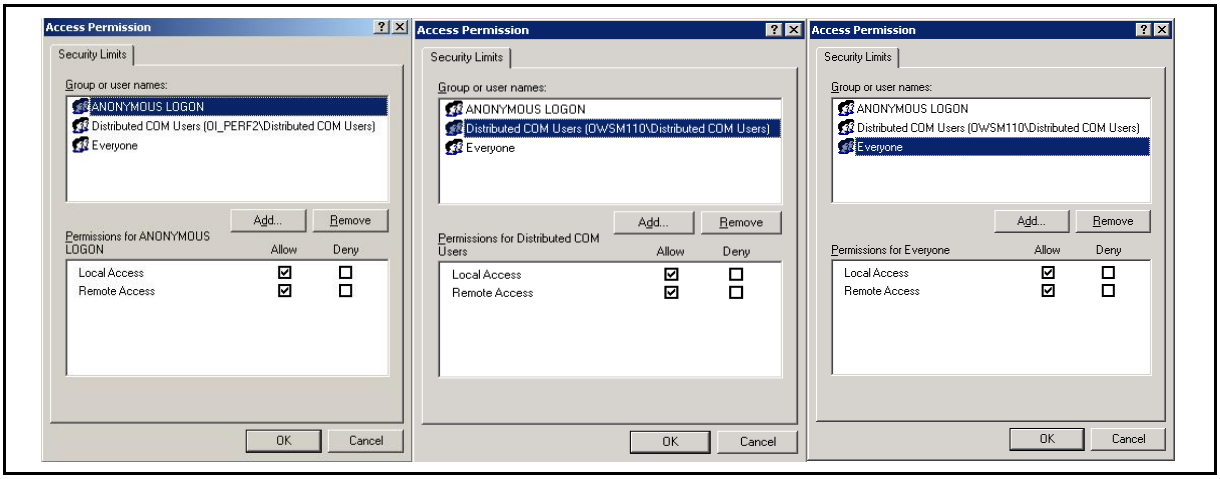
   - Enable Distributed COM on this computer should be CHECKED
   - Default Authentication level should be "Connect"
   - Default Impersonation level should be "Identify"


My Computer
Default Protocols
MSDTC
COM Security
General
Options
Default Properties
Enable Distributed COM on this computer
Enable COM Internet Services on this computer
Default Distributed COM Communication Properties
The Authentication Level specifies security at the packet level.
Default Authentication Level:
Connect
The impersonation level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity.
Default Impersonation Level:
Identify
Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous.
Provide additional security for reference tracking
OK
Cancel
Apply

4. Select the "COM Security" tab and verify the “Edit Limits” for “Access permissions” and for “Launch and Activation Permissions”. These settings control security permissions concerning objects, accessed or launched locally or remotely by PROGRAMS.

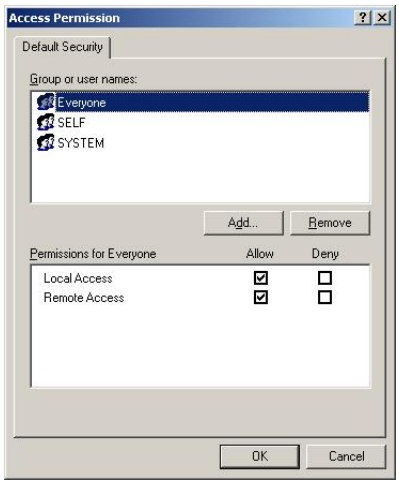

My Computer Properties
General
Options
Default Properties
Default Protocols
MSDTC
COM Security
Access Permissions
You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.
Edit Limits...
Edit Default...
Launch and Activation Permissions
You may edit who is allowed by default to launch applications or activate objects. You may also set limits on appications that determine their own permissions.
Edit Limits...
Edit Default...
OK
Cancel
Apply

5. Click on the "Edit Limits” button in the "Access Permissions" frame. Ensure “ANONYMOUS LOGON”, “Distributed COM Users” and Everyone” groups are present, if not add these groups. Ensure each group has the following permissions.



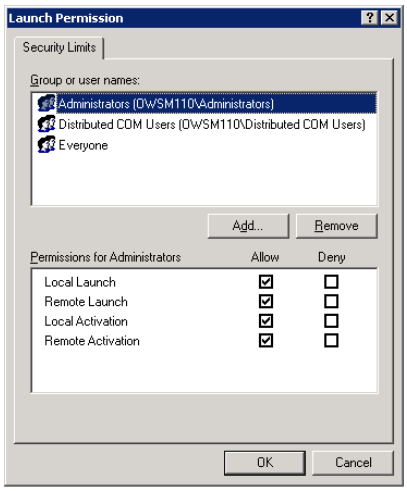
6. Click on the "Edit Default” button in the "Access Permissions" frame. Ensure “Everyone”, “SELF” and “SYSTEM” groups are present. Add these groups, if not there.

7. Ensure each group has the Local and Remote access permissions.

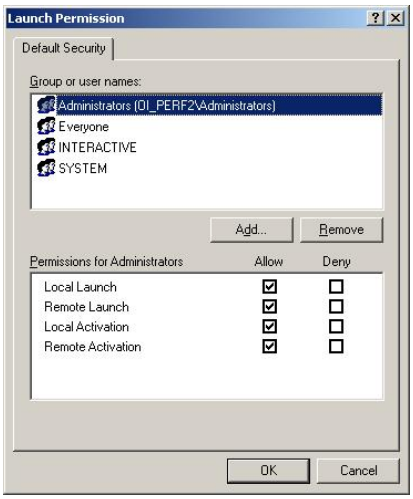


8. Click on the "Edit Limits" button in the "Launch and Activation Permissions" frame. Ensure “Administrators”, “Distributed COM Users” and “Everyone” are present. If not, add these groups.

9. Ensure that each group has the following rights.



10. Click on the "Edit Default" button in the "Launch and Activation Permissions" frame. Ensure that “Administrators”, “INTERACTIVE” and “SYSTEM” groups are present. If not, add these groups. Ensure that “each group has the following rights.



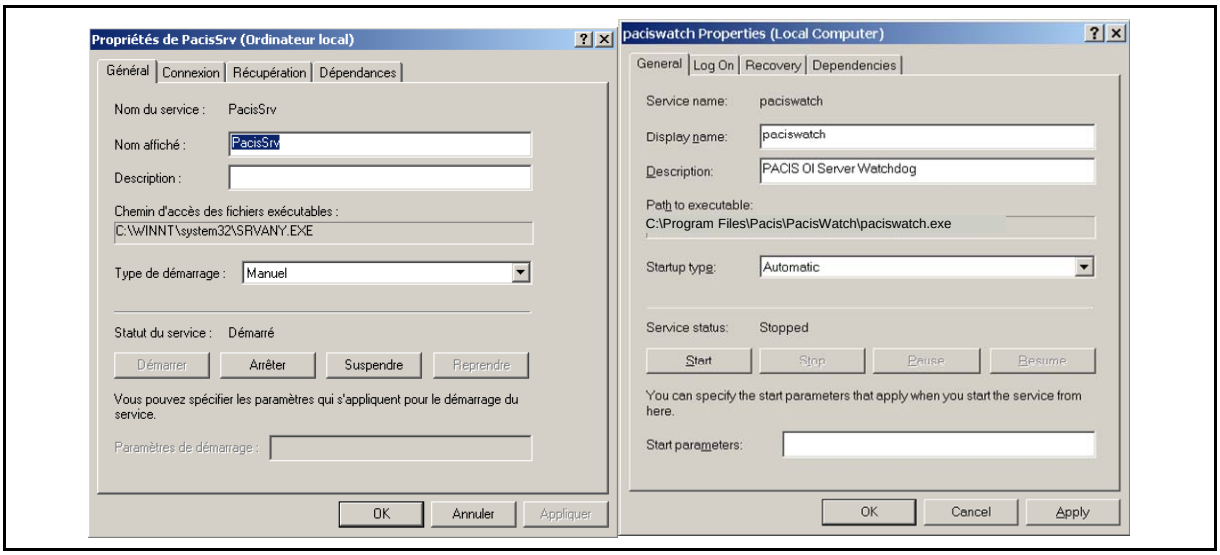
5.3 Application on Windows XP in service mode

5.3.1 Installation

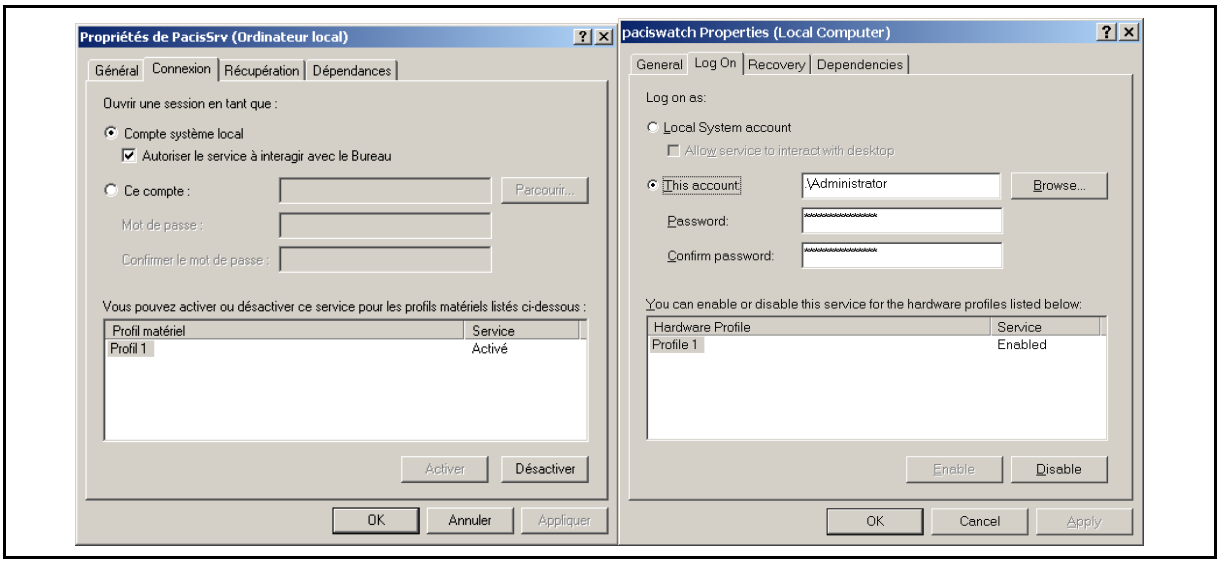
1. Unzip srvany.zip from path %SYSTEMROOT%\system32
2. Copy IntallPacisSrv.bat to Pacis setup folder. Default folder is C:\Program Files\USDATA\S2K\Bin
3. Copy PacisSrvkeys.reg dans to Pacis setup folder. Default folder is C:\Program Files\USDATA\S2K\Bin

5.3.2 Settings

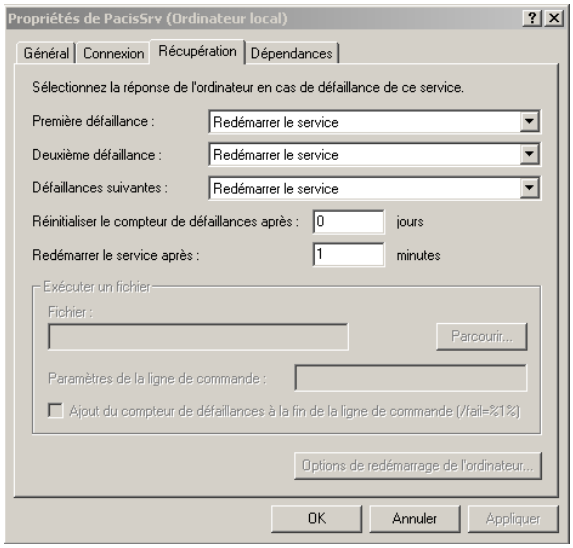
1. Run the command file IntallPacisSrv.bat
2. Open the Service management console
   - Select PacisSrv
   - Access to properties via menu
   - Set the parameters in the General tab



- Set the parameters in the Log on tab



– Set the parameters in the Recovery tab



– No setting in the Dependencies tab

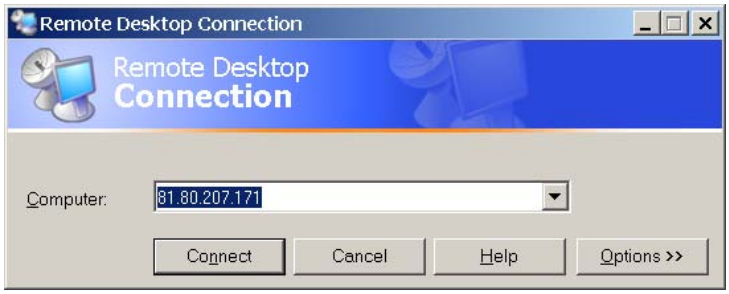
3. Start the PacisSrv service from the services list.

Note: For automatic running of the application, please consult the file sample Demarrage.bat.

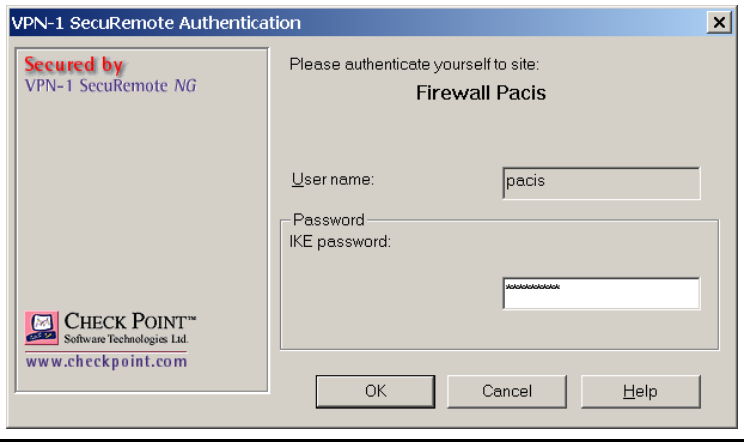
5.4 Launch the application

Launch the WTS client: Start menu/Programs/Accessories/ Communications/Remote Desktop Connection).

Enter the WTS server domain name or IP address:

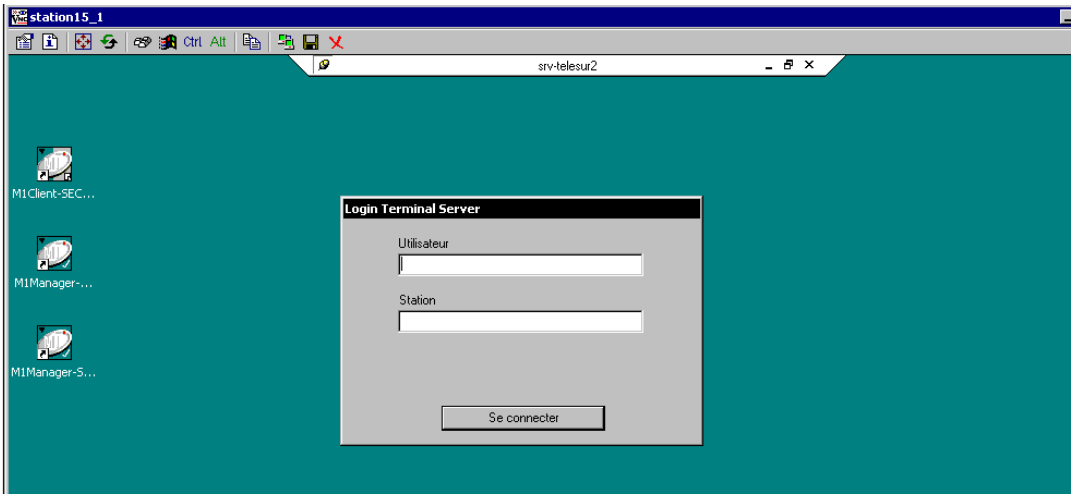


If a VPN is installed, the authentication dialog box is displayed.



Enter the name and the password specific to the VPN site (called “Firewall Pacis” in the example shown) and validate.

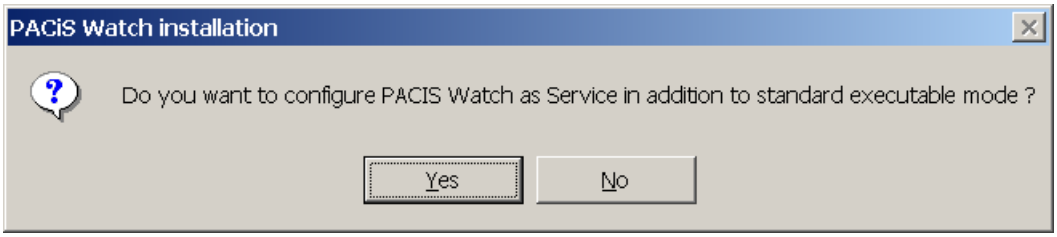
The usual login window is displayed on the WTS client PC.



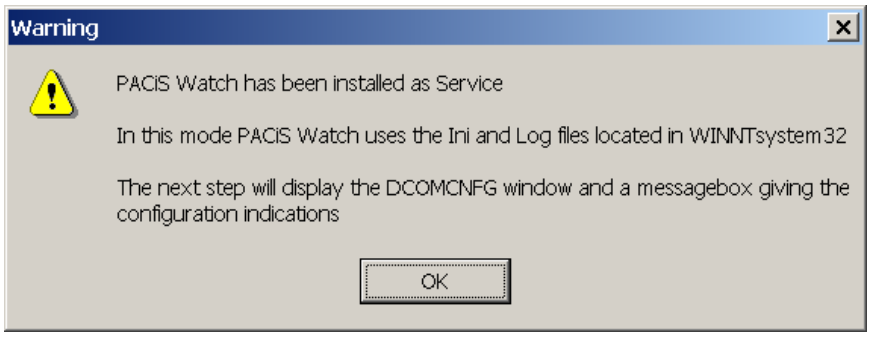
5.5 PACiS Watch in service mode

Note: There is no need to install PACiS Watch in service mode if Windows Server 2003 itself has been installed in this mode.

A dialog box proposes the installation as a service:


PACiS Watch installation
Do you want to configure PACIS Watch as Service in addition to standard executable mode ?
Yes
No

Answering Yes copies the .ini file to the C:\WINNT\system32 folder, because, in service mode, PACiS Watch searches for the .ini file in this folder, instead of the current one, and creates there its log file (paciswatch.txt).

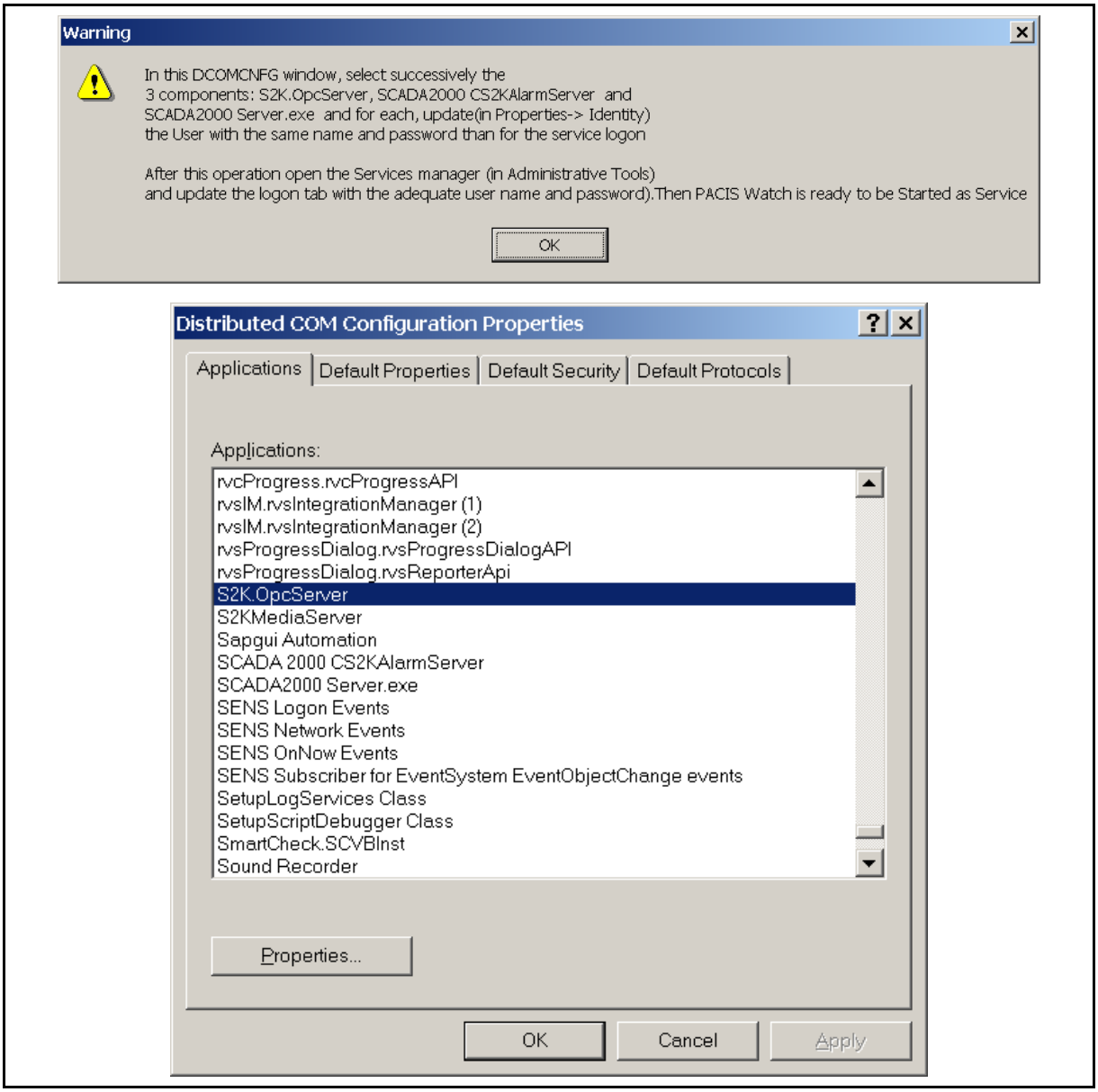

Warning
PACiS Watch has been installed as Service
In this mode PACiS Watch uses the Ini and Log files located in WINNTsystem32
The next step will display the DCOMCNFG window and a messagebox giving the configuration indications
OK

The default paciswatch.ini file has no more SMT_kernel in its “system tools” list, because the use of SMT_kernel is not possible with WTS.

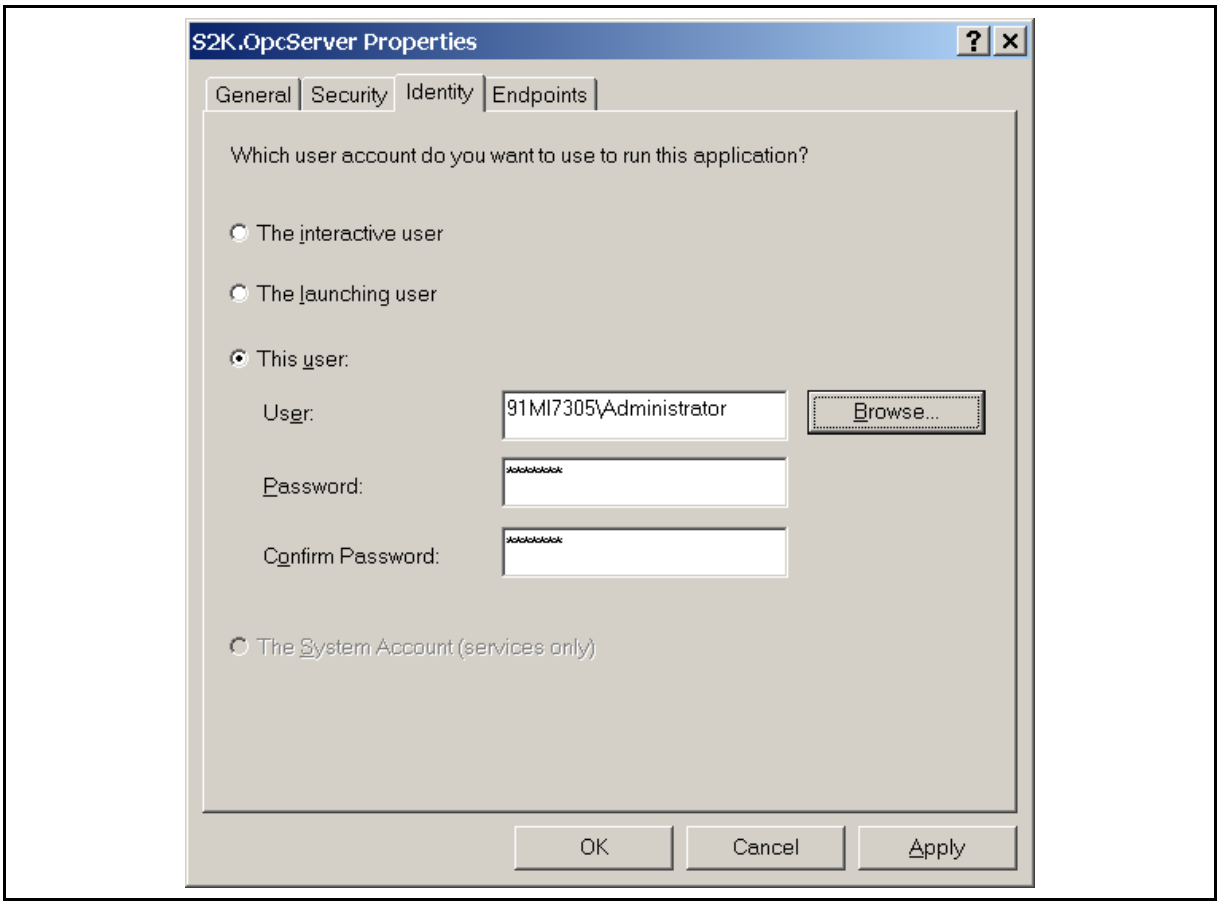
The user can of course add it back if he/she wants to use PACiS Watch as a standard executable (not as service).

5.5.1 Setttings

At the end of the installation of PACIS Watch as a Service the setup launches automatically the dcomcnfg command and guides the user.



In the Properties window, Identity tab, set the same user account used by the service to open a session for the applications S2K.OpcServer, SCADA 2000 CS2KAlarmServer and SCADA 2000Server.exe.



The same account will be chosen for the configuration of PacisWatch in the service manager (see next paragraph).

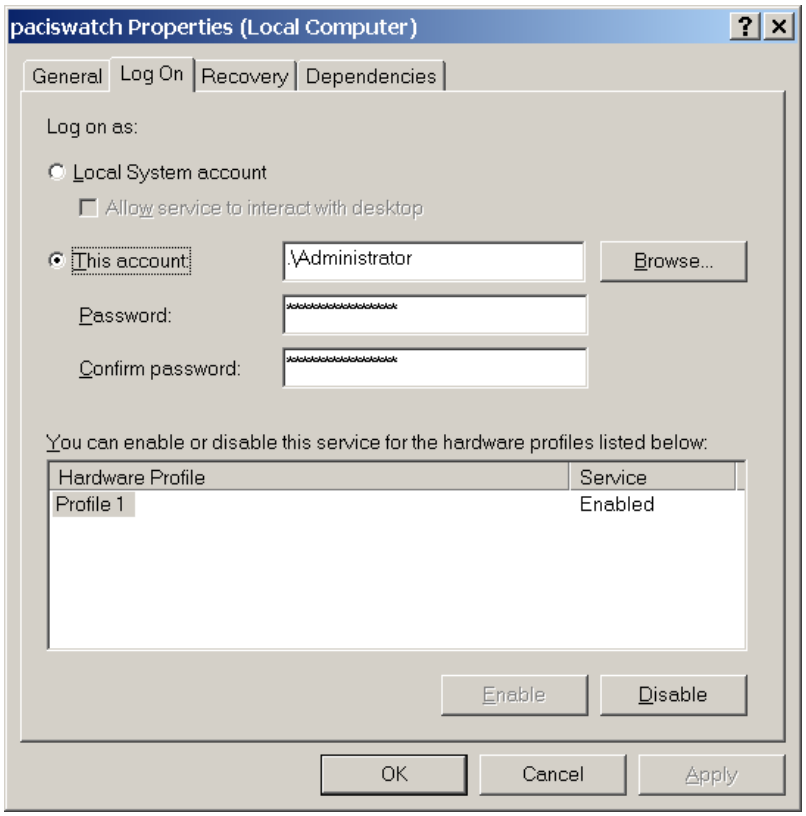
Type your password twice for each of these executables.

Note: To launch the Services manager manually, run dcomcnfg.

5.5.2 Settings as a service

Open the Control Panel / Administration Tools / Services; this displays Paciswatch in the services list (potentially after refreshing the list).

On the Paciswatch service, right click Properties and select the user account used by the service to open a session.

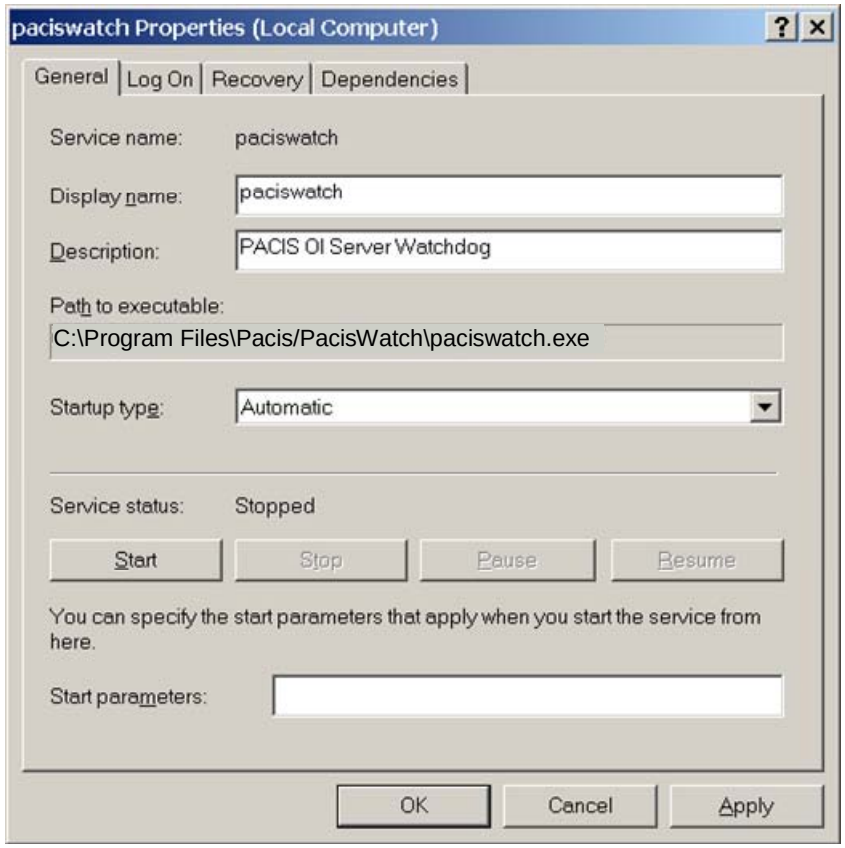


1. Under Log On tab, click on This account, then choose the same account with administrative rights than the one configured in paciswatch service properties..
2. Using the Browse button, click on the domain or the work group of the wished user or group.
3. In the list Name, click on the user or group account, or enter the name of account in the area Name, then click on OK.
4. In the fields Password and Confirm the password, type the password of user account.

The user account that you select should be created in the local users and local groups of the PC Management tool, specifically to log onto the service. In the area User properties, make sure that the option 'The password never expires' is enabled for the user account and that this account is member of the appropriate groups.

Select the Automatic option in the Startup type field (in the General tab). This allows this service to start automatically after a PC reboot as soon as Windows starts.

If applicable, remove the shortcut to PACiS OI in the Start/Programs menu.



In manual mode, PACiS Watch must be started and stopped via the Windows services manager).

6. NETWORKS INSTALLATION

Systems are based on networks. Practice shows that lot of troubles (even after some time) come from incorrect installation of the networks. Here are referenced some installation practices in three sub-chapters for each kind of functional network

- L-BUS: Legacy Bus between Computer and IED on field bus
- S-BUS Station Bus between PACiS devices and other IED based on Ethernet with IEC 61850 protocol.
- T-BUS: Telecontrol BUS between system and Remote Control Point or SCADA

6.1 Legacy Bus installation

Installation of Legacy Bus or field Bus is described in computer IN chapter. Cable definition and maximum length is defined in chapter CO (Connection)

Two kinds of cable can be used with copper and optical. Installation common problem are slightly different.

Copper cables are installed in daisy chain with computer usually in one extremity. For RS422 and RS485 links terminal resistor (150 ohms) has to be installed at both ends. When LBUS is connected on computer BIU a jumper on the board can put a calibrated resistor for LBUS end. Another common installation problem is that LBUS cable is correctly protected from perturbation: not correctly shielded at both end, and/or installed into cubicle in contact with CT/VT or power digital signal.

Optical connection is done point to point. Optional box allows to make kind of Hubb (several input/output). The common trouble is that fiber bending under a 15cm radius raise permanently signal attenuation until glass breaking. With time and electromagnetic field the glass attenuation raises a bit, then signal level over attenuation leads to perturbation in communication.

6.2 Station Bus installation

Installation of Station Bus based on Ethernet is lightly described in all PACiS devices IN chapters, and more in detail into IN chapter of MiCOM Hxxx range devices.

The Ethernet network is composed of cables and switches (possibly repeaters). The network scheme ask as mandatory define cable length, physical layer, speed. The chapter CO of MiCOM Hxxx range devices and MiCOM C264 computer defines cable characteristic (example class 5 for 100T). PACiS system has defined a range of network switch defined in MiCOM Hxxx range devices and MiCOM C264 documentation (chapter HW & FT) with number of connection and power voltage.

Copper cable installation problems come often from cable quality compared from environment (class, shielding, protection against animal). For optical cable the handling during installation is a standard problem to not bend or even break glass. Especially with glass fiber shelding is recommended especially for mice. Optical cable has emitter/receiver fibers to clearly distinguish before starting the install. As remind in SA chapter glance into fiber can damage eye and specific tool is recommended to commission one by one the fiber.

PACiS provides via specific switch a redundant Ethernet. Because it is redundant a single test can hide a wrong installation of master/secondary network. It is recommended to make commissioning after each switch installation and not globally.

6.3 Telecontrol Bus installation

Two PACiS devices Computer or gateway can have connection to SCADA via S-BUS. The basic installation is described into their IN chapter.

In both case TBUS communication might need a modem to get into PSTN or RNIS networks. Modems are country dependant and not part of the system. Modems should be configurable for all communication parameters.

7. NON PACiS DEVICES INSTALLATION

7.1 PACiS OI printer

In standard installation PACiS OI printers are installed on same OWS that the server part of PACiS OI. Printer has normally to be powered and connected before starting installation to use “Plug in” and automatic detection during driver installation on PC.

Using Microsoft Windows™ 2003 or XP Parameters/Printer makes a standard “Add Printer” to start windows installer assistant. Assistant proposes a kind of printer:

- local (OWS serial port) and the printer driver is installed from printer manufacturer or
- network (browse then OWS neighbouring to found network printer).

Printer name should match the associated attribute name in database, and it has to be defined as default printer.

Network printer can be a printer managed by and other PC. If the network PC is not Microsoft Windows™ 2003 or XP, PC installation of printer on network PC suppose to install printer as local on LPT, then to add a second “local port” on network PC for the remote access.

When printer is defined it needs to be configured. Select the printer, right click on property and select the thumb Ports. Chose in the list the selected port and double click. Define “local port” and enter its network/alias name then tick the printer in list and leave Port menu by Ok.

7.2 MiCOM C264 printer

Printer directly on MiCOM C264 computer has its installation fully described in computer IN chapter.

Printer is a serial 7-bit printer RS232C for listing. It can be installed later on one free port among four of the computer. Data printed are defined in database. It is important to notice in this installation that a file has to be copied into the computer (defining used port, and communication speed).

7.3 PACiS System Master clock

The external master clock receives absolute time synchronisation. In PACiS case, the standard means is to receive the absolute time synchronisation from GPS (Global Positioning Satellite system). This may be done with Hopf radio clock.

Installation of ***Hopf*** device is described in detail in its documentation. It is based on the ***Hopf*** 6870 GPS radio clock as a separate device that transmits time synchronisation via IRIG-B signal.

The electronic device has link to antenna and maintenance software. Antenna should be installed on building top to see maximum of GPS satellites (4 or more). Care should be taken during this operation on roof against fall and possible power line neighbouring. Special protection against thunder lightning should be taken (at antenna neighbouring and limited distance from all electronic devices to common ground usually 10m). Link between antenna and ***Hopf*** radioclock is made by 25 meter cable (70m can be reach with another special cable after line amplifier should be added).

Maintenance software helps to commission correct detection of position then time, and definition of transmitted synchronisation.

Hopf 6870 should be powered 18-60V DC.

Once the hardware is installed, and maintenance software has been used to configure synchronisation, save the set-up and install system synchronisation.

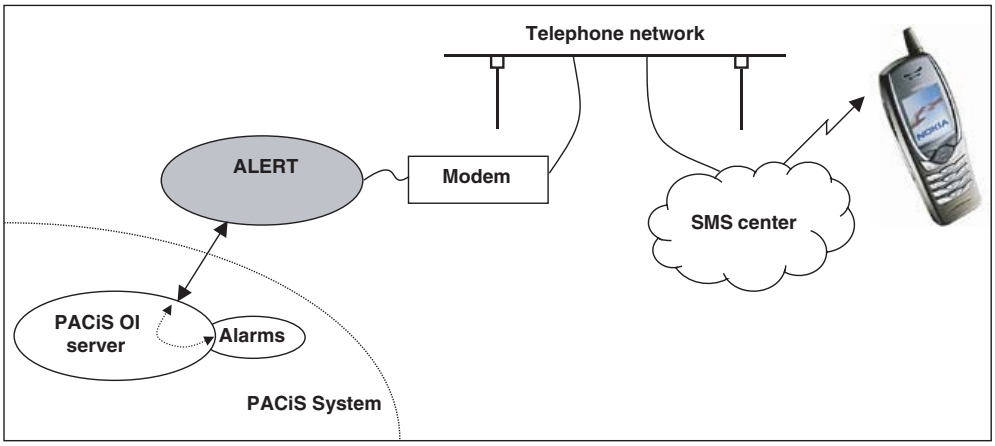
The time synchronisation scheme is to distribute the IRIG B synchronisation to one MiCOM Computer C264 with IRIG B based on BNC cable, T, and 50ohms impedance termination. This computer will then synchronise the other SBUS equipment through the Ethernet network.

8. NON PACiS APPLICATIONS INSTALLATION

8.1 ALERT Software

The ALERT software is used for alarm notification into PACiS.

MICROMEDIA International produces the ALERT software.

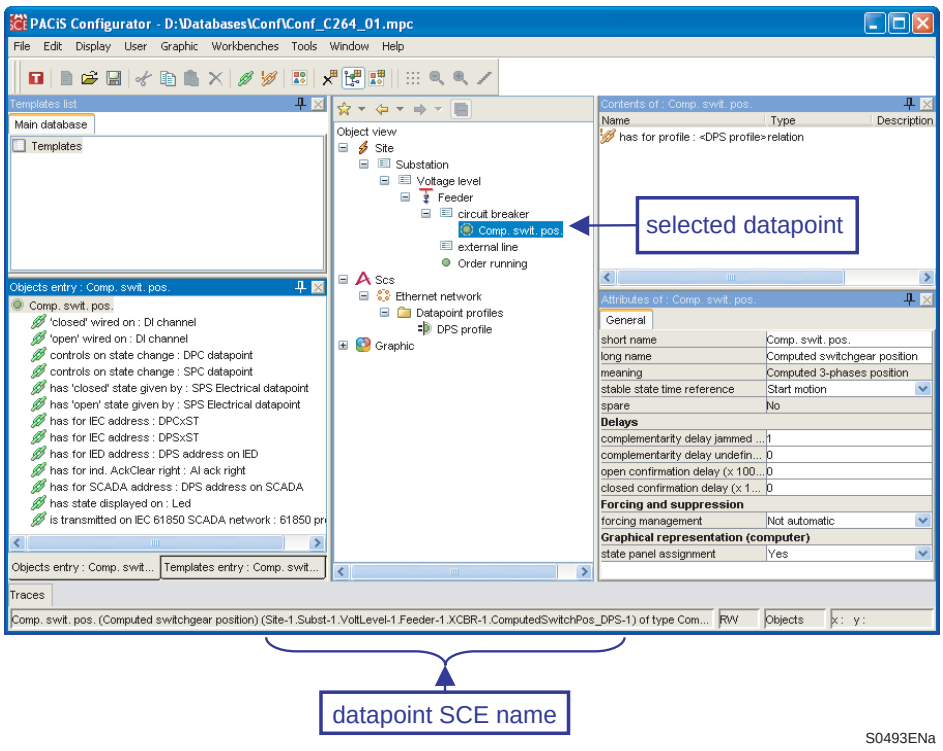


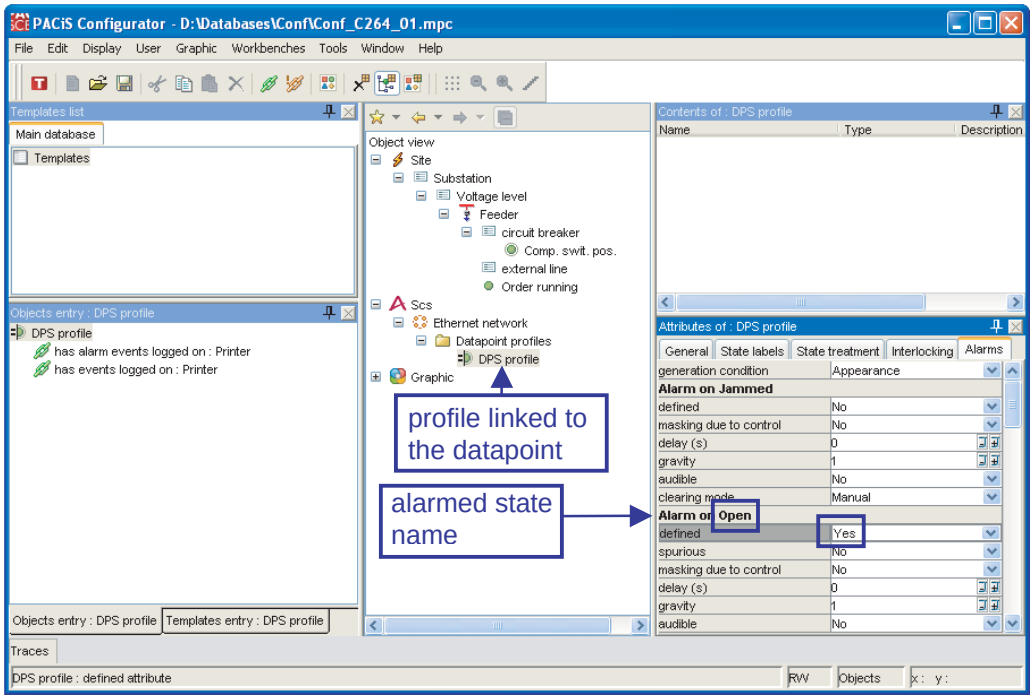
ALERT supervises and manages a list of application variables on the PACiS OI Server. The variables declared in this list are [Object Linking and Embedding (OLE)] [for Process Control (OPC)] variables. ALERT polls their current state.

8.1.1 Identification of the PACiS alarms to be notified

Use the SCE to retrieve the name of the OPC variable that corresponds with the alarm to be notified.

During this phase you will manually collect the list of the alarms to be notified, and write them in an ASCII file, for example. This can be useful as we will see later.


PACiS Configurator - D:\Databases\Conf\Conf_C264_01.mpc
File Edit Display User Graphic Workbenches Tools Window Help
Templates list
Main database
Templates
Object view
Site
Substation
Voltage level
Feeder
circuit breaker
Comp. swit. pos.
external line
Order running
Scs
Ethernet network
Datapoint profiles
DPS profile
Graphic
selected datapoint
Contents of : Comp. swit. pos.
Name Type Description
has for profile : <DPS profile>relation
Attributes of : Comp. swit. pos.
General
short name Comp. swit. pos.
long name Computed switchgear position
meaning Computed 3-phases position
stable state time reference Start motion
spare No
Delays
complementarity delay jammed ... 1
complementarity delay undefin... 0
open confirmation delay (x 100... 0
closed confirmation delay (x 1... 0
Forcing and suppression
forcing management Not automatic
Graphical representation (computer)
state panel assignment Yes
Objects entry : Comp. swit. pos.
Comp. swit. pos.
'closed' wired on : DI channel
'open' wired on : DI channel
controls on state change : DPC datapoint
controls on state change : SPC datapoint
has 'closed' state given by : SPS Electrical datapoint
has 'open' state given by : SPS Electrical datapoint
has for IEC address : DPCxST
has for IEC address : DPSxST
has for IED address : DPS address on IED
has for ind. AckClear right : AI ack right
has for SCADA address : DPS address on SCADA
has state displayed on : Led
Objects entry : Comp. swit...
Templates entry : Comp. swit...
Traces
Comp. swit. pos. (Computed switchgear position) (Site-1.Subst-1.VoltLevel-1.Feeder-1.XCBR-1.ComputedSwitchPos_DPS-1) of type Com...
RW
Objects
x : y :
datapoint SCE name
S0493ENa



S0494ENa

The OPC name of an alarm is: <datapoint SCE name>.<alarmed state name>

In our example it is:

Site-1.Subst-1.VoltLevel-1.Feeder-1.XCBR-1.ComputedSwitchPos_DPS-1.Open

It relates to the PACiS OI alarm on the opened state of the datapoint.

NOTE: you must be aware on how alarms are managed:

⇒ In the STATE BASIS mode, all the defined alarms are visible as different items as presented above. According to the example, you will see the "...**DPS-1.Jammed**" and "...**DPSP-1.Open**" items.

⇒ In the DATA BASIS or GRAVITY BASIS, only the first state is visible as an OPC item. According to the example, you will see only the "...**DPS-1.Open** item.

8.1.2 Connection between ALERT and PACiS alarms

This phase occurs at run-time, when both the PACiS OI server and ALERT have been launched.

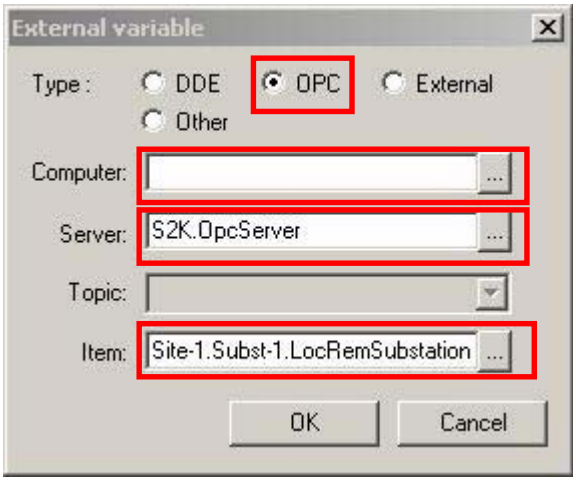
NOTE: ALERT may be started automatically by the way of Windows/Start/Program/Startup.

The main activity consists in setting in ALERT the list of PACiS alarms to be notified. Here, the name described in §7.2 is used.

ALERT allows to enter 'Tags' (refer to the ALERT user manual for detailed information on how to configure it). In our case they correspond to the PACiS alarms.

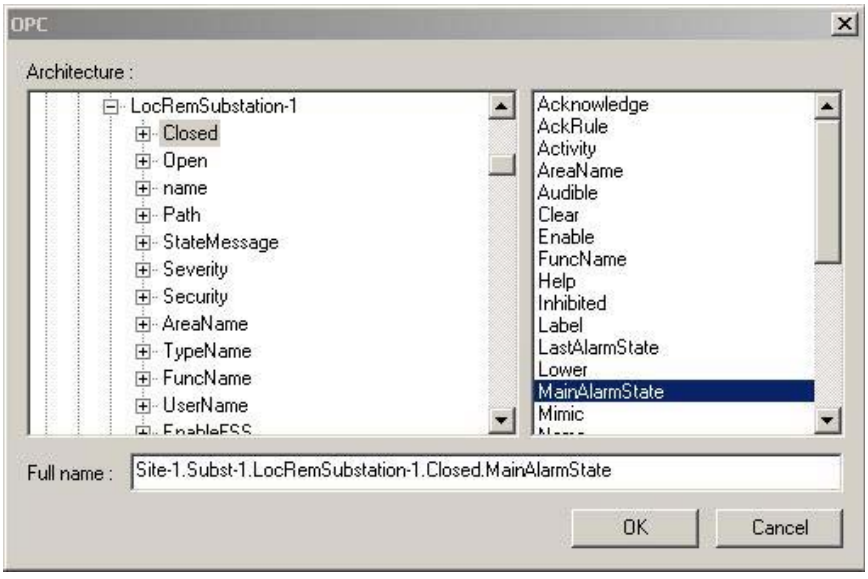
For all 'Tags':

- add a tag



- select OPC
- computer: name of computer which supports the OI server
- server: always S2K.OpcServer
- item: 2 ways are possible to enter the item name:

  1. using the created ASCII file (see § 9.1), add **.MainAlarmState** at the end of each OPC variable in the ASCII file, then copy each line in the Item box
  2. using the ALERT browser:

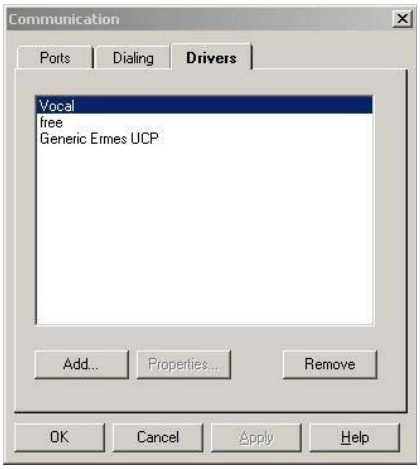


8.1.3 ALERT configuration for SMS

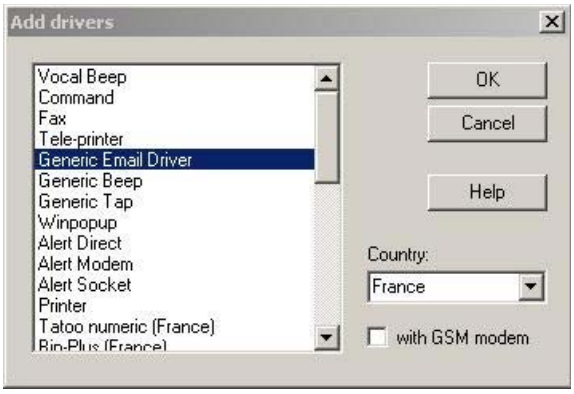
Here is described the case of SMS sent through e-mail using SMSToB service in France (www.smstob.com). A lot of services are available, depending on the country in which PACiS is used.

8.1.3.1 Driver configuration

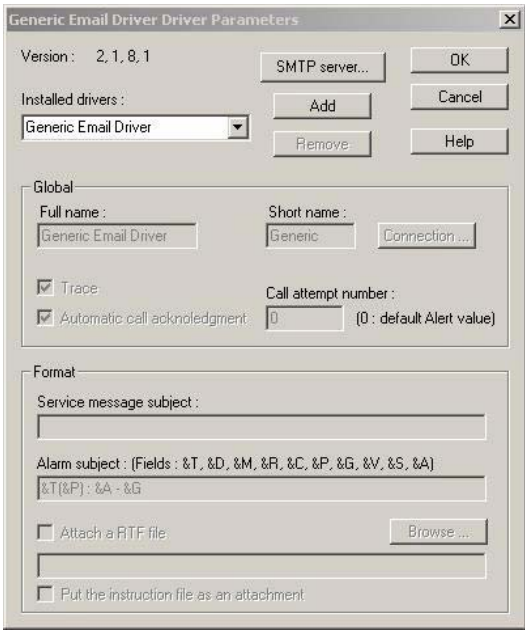
- select the “configuration / communication” menu
- select "drivers", click on "Add…"



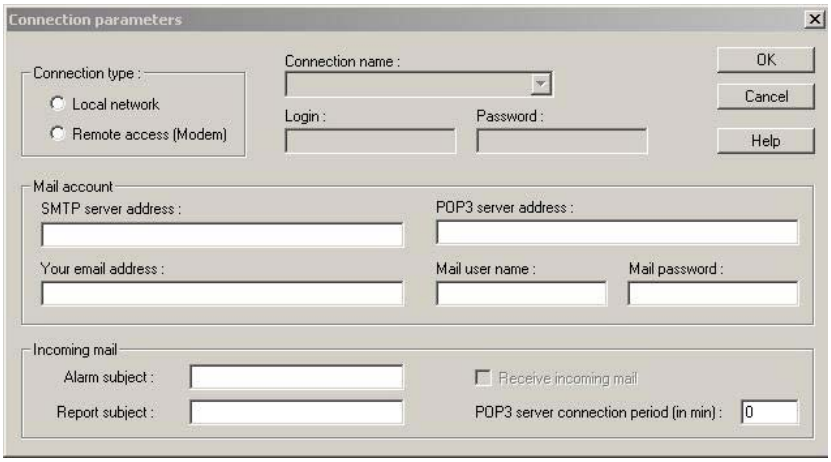
- select country and driver type (generic email driver)



- select created driver et click on “Properties...”



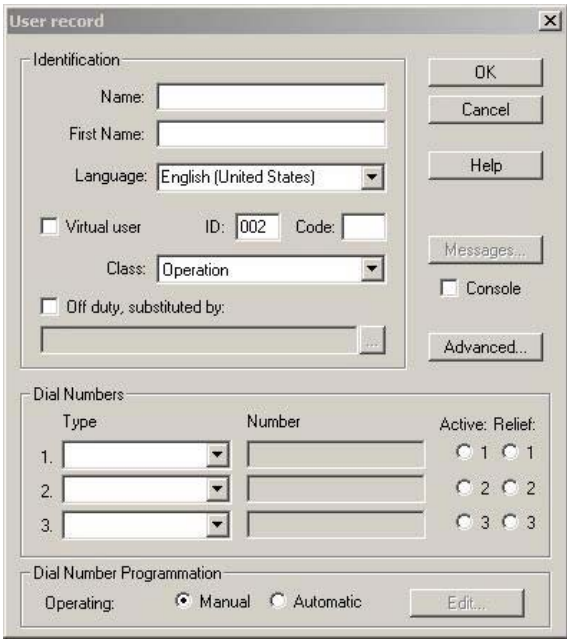
- click on “Add...”. In Global part click on “Connection ....”



- define all parameters attached to your Internet access (warning: the e-mail address must be the same than the address used to have an account on SMSToB service)
- in Format part ; alarm subject: remove all fields

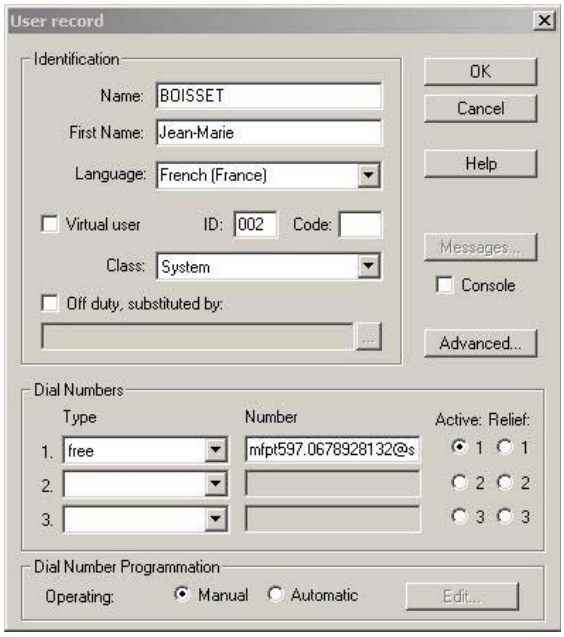
8.1.3.2 User definition

- add a user

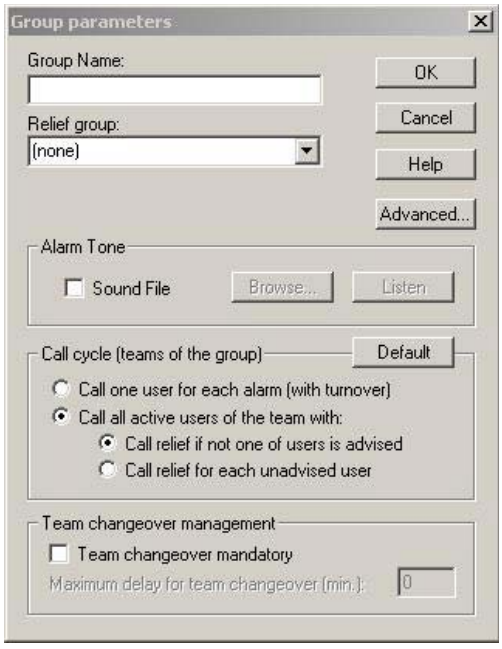


- type the name, the first name, the language, the class

- in “Dial Number” part, line 1:



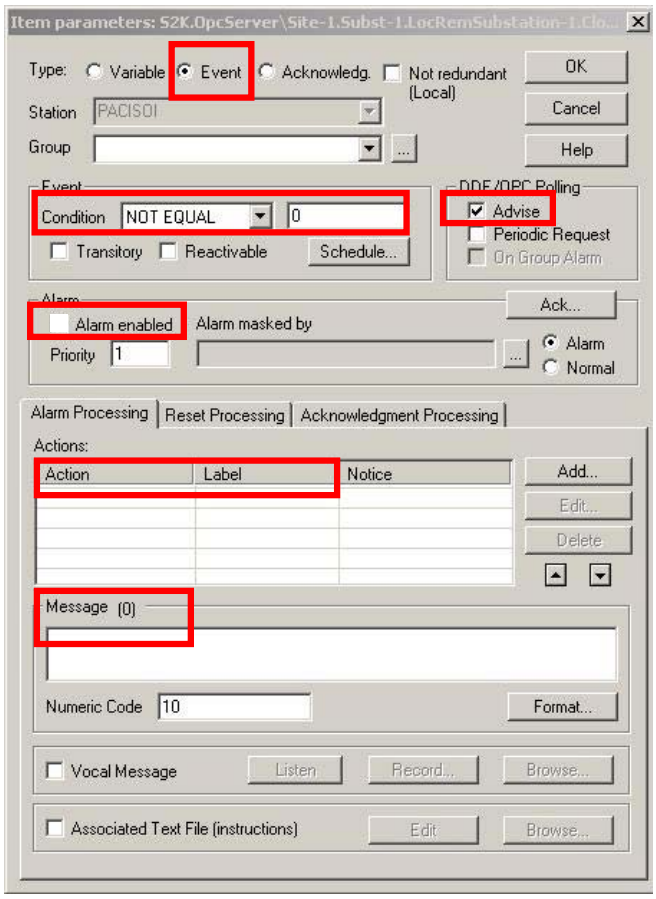
  - type: select the driver you have created
  - number: <password>.<phone number>@smstob.com
- you can define several user if several people have to receive a SMS when an alarm occurs
- if the same action (i.e. send the same SMS) must be performed when an alarm occurs, the users can be attached to a group:
  - add a group



  - define the group name
  - select "call all active users of the team"
  - drag and drop users to the group

8.1.3.3 Tag properties

For each tag (cf. § 9.2), you have to define the properties:



Type = event

Alarm = not enabled

DDE/OPC polling = Advise

Condition should be defined depending on what the user wants. The values of the alarm tag are:

Alarm state	Value
NO_SIGNIFICANT	0
DISABLED	1
INACTIVE	2
INACTIVE_ACK	6
ACTIVE_ACK	8
INACTIVE_UNACKI	18
INACTIVE_UNACKA	34
ACTIVE_UNACK	40

If the user wants to receive a SMS each time an alarm becomes active unacknowledged, the condition will be “EQUAL 40”.

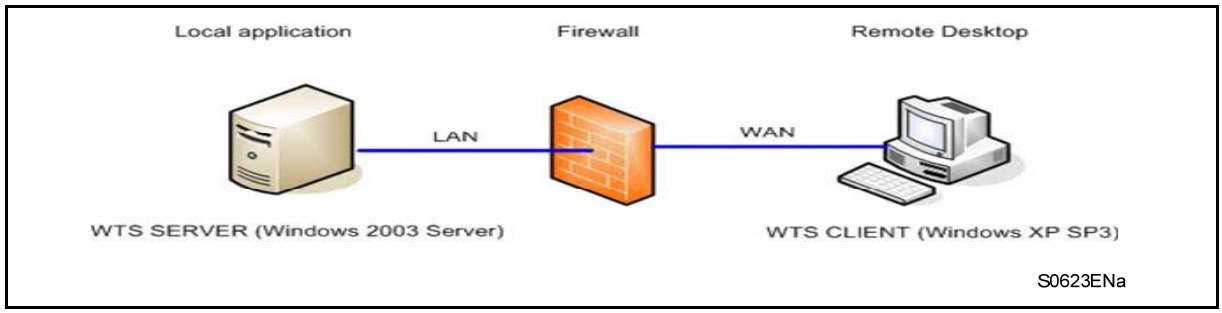
Alarm processing = click on "add" – The action can be “call user” or “call group” depending on the user definition

Message = the button “Format…” allows to define the SMS message.

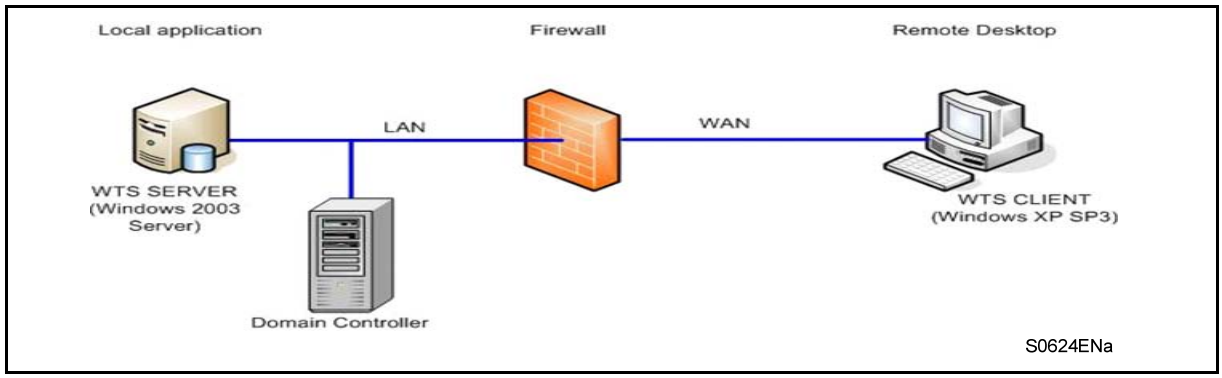
8.2 Setting up a remote terminal (Windows Terminal Service)

8.2.1 Architectures

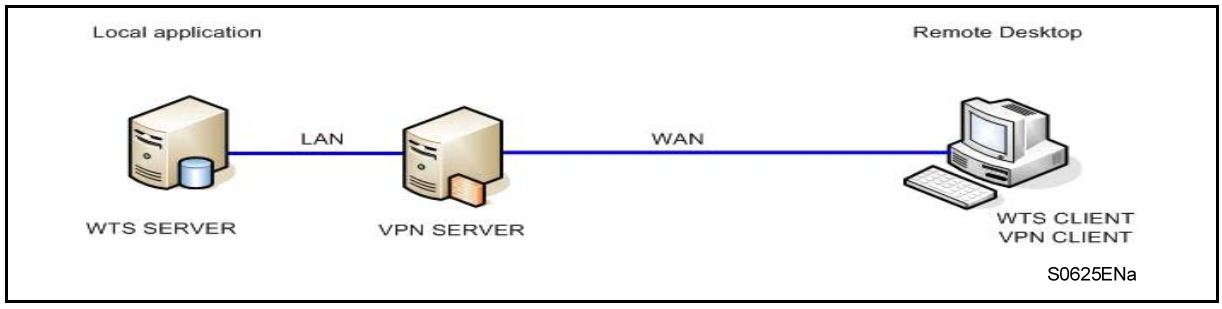
Basic:



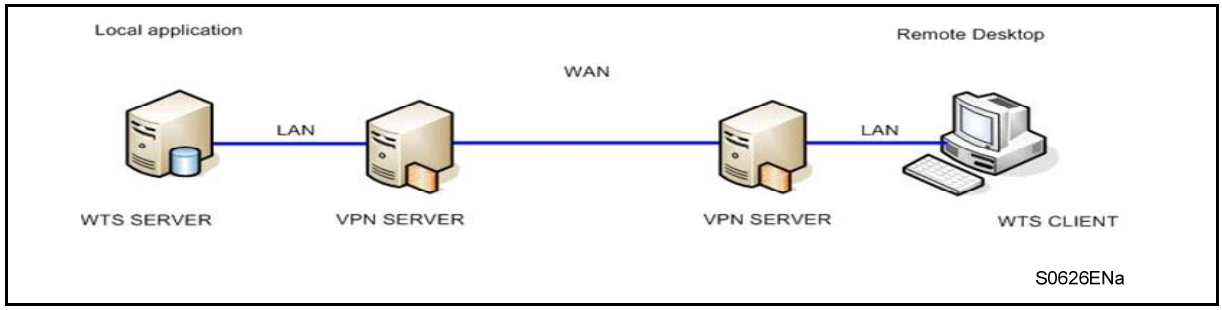
With a Domain Controller:



VPN: the client stations are members of a virtual LAN based on address translation (NAT)



Two VPN servers:



8.2.2 WTS Server installation (Windows Server 2003)

The server must be installed with the Terminal Server role

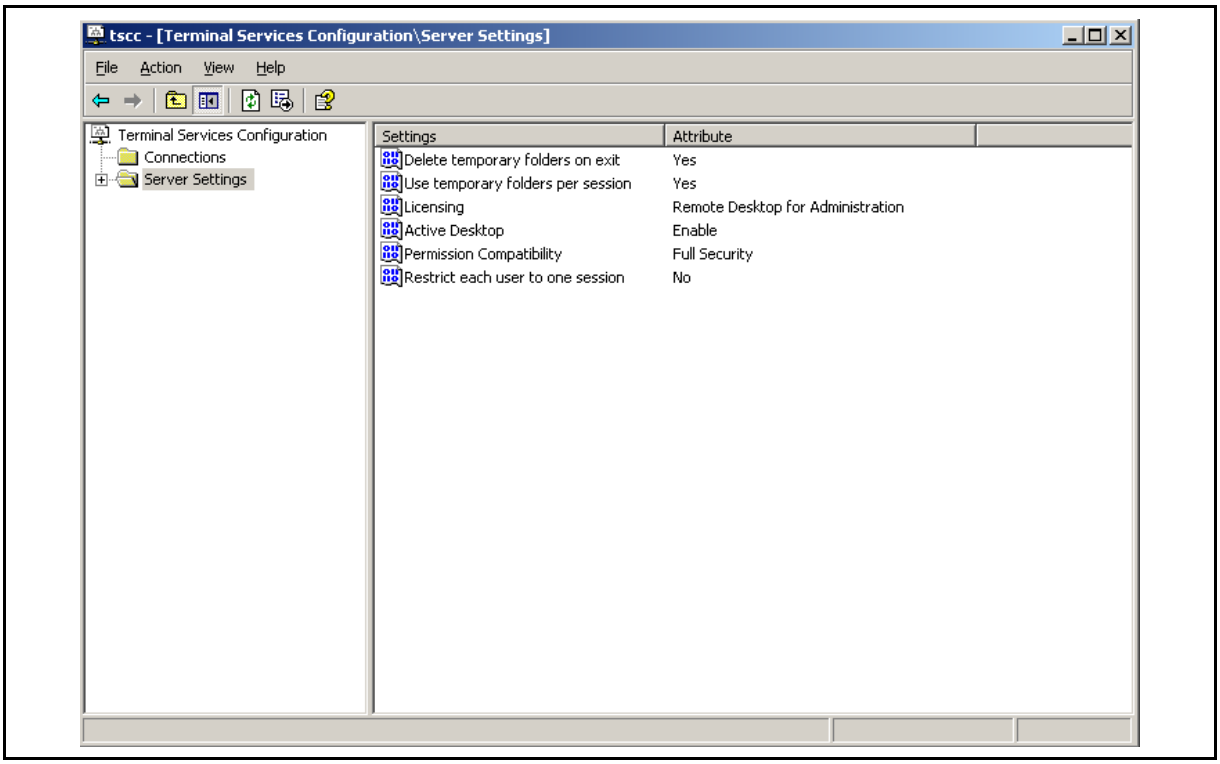
- either through the link Manage your server in the Start menu: select Terminal Server
- or through the Control Panel/Add or remove a component: check Terminal Server in the list and complete the installation

8.2.3 Terminal Server services configuration (Windows Server 2003)

8.2.3.1 Console (operation and group permissions)

Open the console using Administration tools > Terminal Server configuration.

Click RDP-Tcp to open the Properties window.



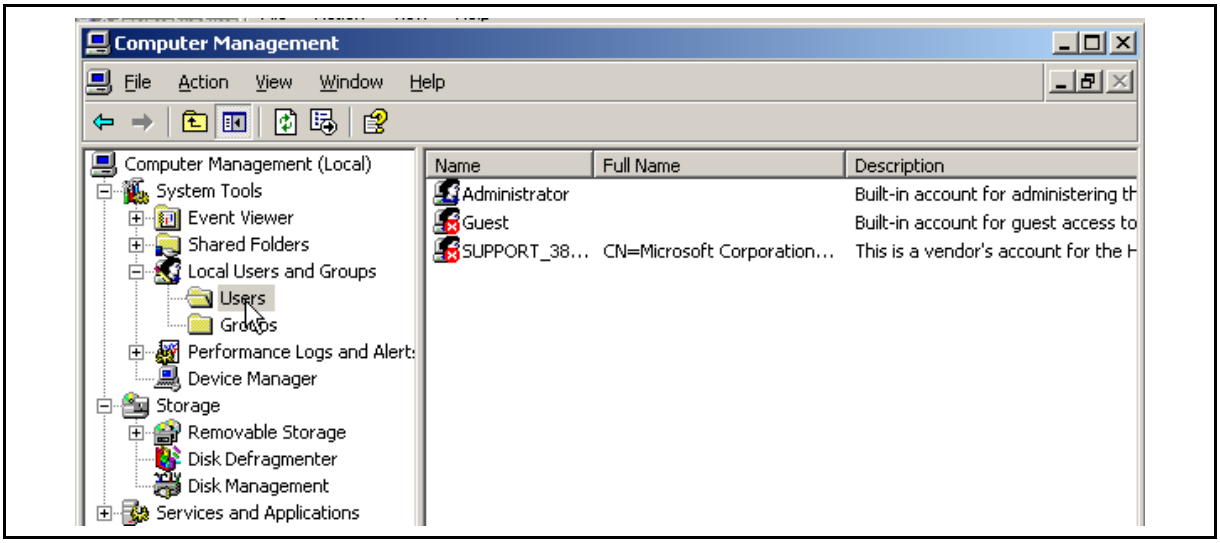
In the Connections node, configure the connection operation and the permissions of the group Remote Desktop Users.

In the Server Settings node, various options are available (Active desktop, …).

For details, refer for example to http://www.laboratoire-microsoft.org/articles/win/tse2003.

8.2.3.2 Users properties

Select the server icon. Right-click Manage; a console shows:

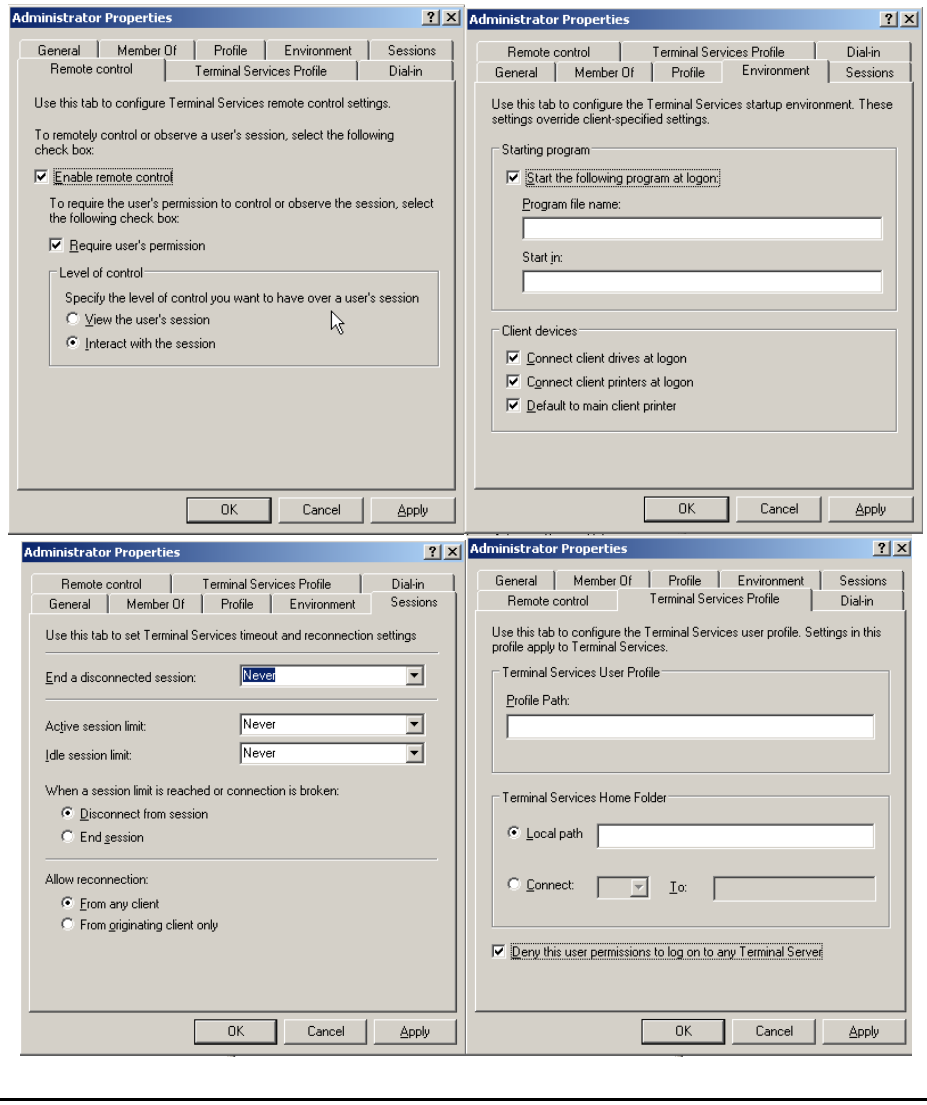


To display the users list, click Local Users and Groups / Users.

Select a user.

To display the user's properties, right-click Properties.

Fill in the tabs that follow:

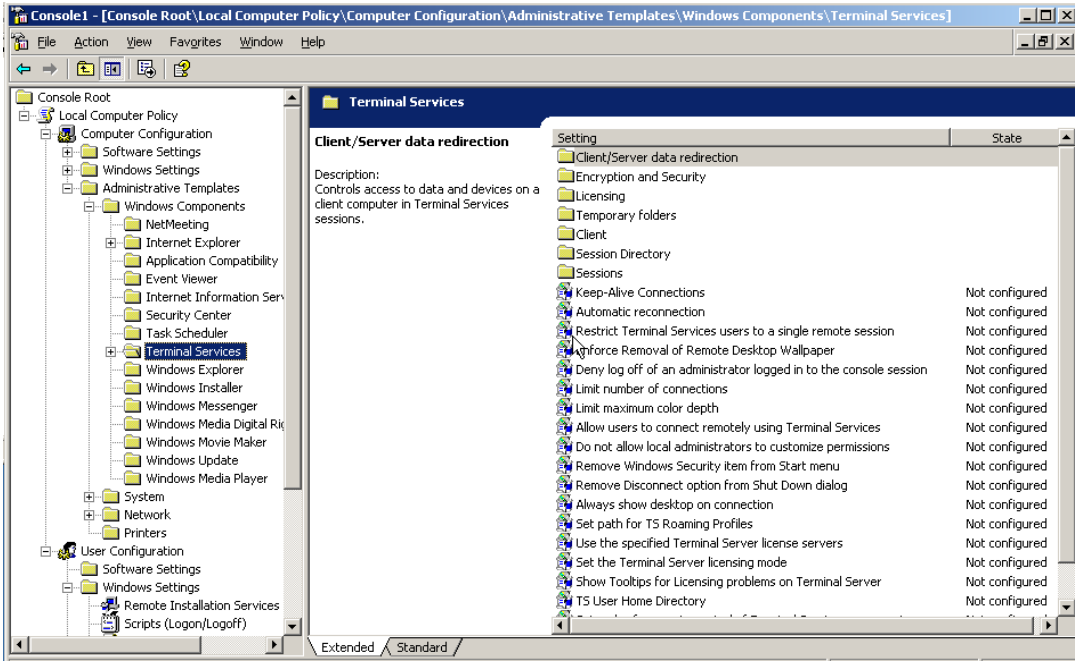

Administrator Properties
General
Member Of
Profile
Environment
Sessions
Remote control
Terminal Services Profile
Dial-in
Use this tab to configure Terminal Services remote control settings.
To remotely control or observe a user's session, select the following check box:
Enable remote control
To require the user's permission to control or observe the session, select the following check box:
Require user's permission
Level of control
Specify the level of control you want to have over a user's session
View the user's session
Interact with the session
OK
Cancel
Apply
Use this tab to configure the Terminal Services startup environment. These settings override client-specified settings.
Starting program
Start the following program at logon:
Program file name:
Start in:
Client devices
Connect client drives at logon
Connect client printers at logon
Default to main client printer
Use this tab to set Terminal Services timeout and reconnection settings
End a disconnected session:
Never
Active session limit:
Idle session limit:
When a session limit is reached or connection is broken:
Disconnect from session
End session
Allow reconnection:
From any client
From originating client only
Use this tab to configure the Terminal Services user profile. Settings in this profile apply to Terminal Services.
Terminal Services User Profile
Profile Path:
Terminal Services Home Folder
Local path
Connect:
To:
Deny this user permissions to log on to any Terminal Server

Make sure the box 'Deny this user permissions to log on to any Terminal Server' is NOT checked (Terminal Services Profile tab).

8.2.3.3 Policies

- Click Start, click Run, and in the text box, type mmc /s and then click OK.
- From the Console menu, select Add/Remove Snap-in, and click the Add button.
- From the Available Standalone Snap-in list, select Group Policy, and click the Add button.
- In the wizard, select the local computer and click Finish.
- In the list, click Close.
- In the Add window, click OK.

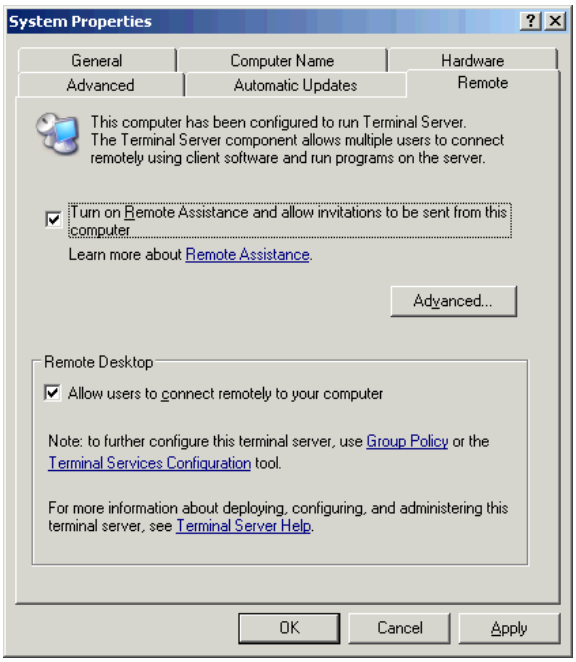
This grants access to the Local Computer Policy, that allows to configure all the users interfaces: in the Default Domain Controllers Policy console, expand Computer Configuration; navigate to Administrative Templates Settings, then to Windows Components, and select Terminal Services:


Console1 - [Console Root\Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\Terminal Services]
File Action View Favorites Window Help
Console Root
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Windows Components
NetMeeting
Internet Explorer
Application Compatibility
Event Viewer
Internet Information Ser
Security Center
Task Scheduler
Terminal Services
Windows Explorer
Windows Installer
Windows Messenger
Windows Media Digital Ri
Windows Movie Maker
Windows Update
Windows Media Player
System
Network
Printers
User Configuration
Software Settings
Windows Settings
Remote Installation Services
Scripts (Logon/Logoff)
Terminal Services
Client/Server data redirection
Description:
Controls access to data and devices on a client computer in Terminal Services sessions.
Setting
State
Client/Server data redirection
Encryption and Security
Licensing
Temporary folders
Client
Session Directory
Sessions
Keep-Alive Connections Not configured
Automatic reconnection Not configured
Restrict Terminal Services users to a single remote session Not configured
Enforce Removal of Remote Desktop Wallpaper Not configured
Deny log off of an administrator logged in to the console session Not configured
Limit number of connections Not configured
Limit maximum color depth Not configured
Allow users to connect remotely using Terminal Services Not configured
Do not allow local administrators to customize permissions Not configured
Remove Windows Security item from Start menu Not configured
Remove Disconnect option from Shut Down dialog Not configured
Always show desktop on connection Not configured
Set path for TS Roaming Profiles Not configured
Use the specified Terminal Server license servers Not configured
Set the Terminal Server licensing mode Not configured
Show Tooltips for Licensing problems on Terminal Server Not configured
TS User Home Directory Not configured
Extended Standard

8.2.4 Users statement in Active Directory

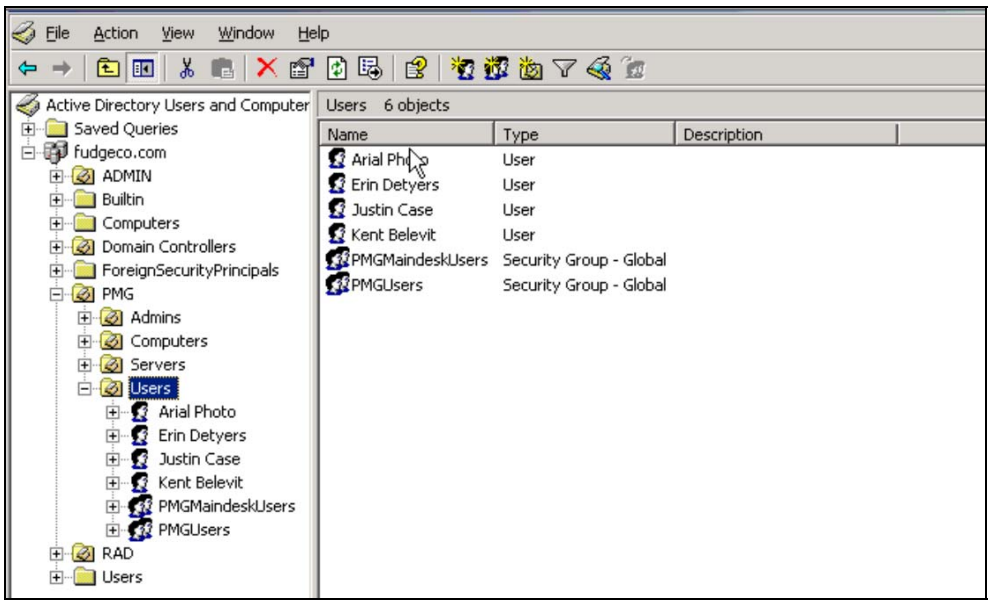
The server runs Terminal Services.

To activate the remote desktop, select Control panel/System/Remote and tick the box ‘Allow users to connect remotely to your computer’:

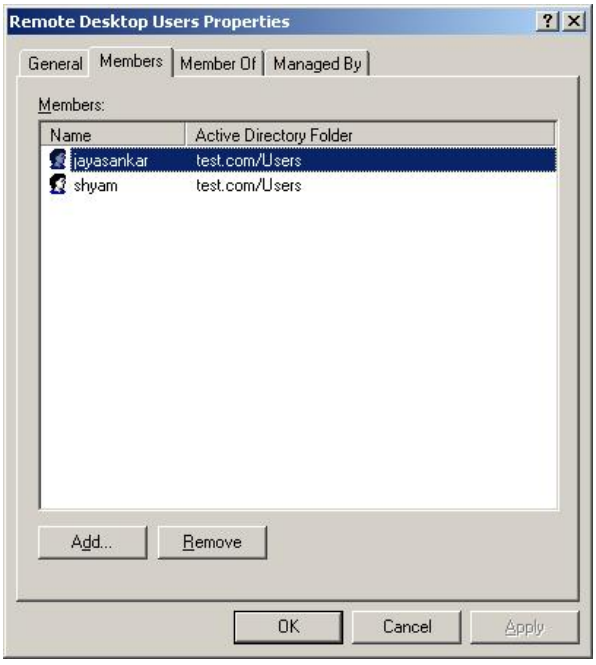

System Properties
General
Computer Name
Hardware
Advanced
Automatic Updates
Remote
This computer has been configured to run Terminal Server.
The Terminal Server component allows multiple users to connect remotely using client software and run programs on the server.
Turn on Remote Assistance and allow invitations to be sent from this computer
Learn more about Remote Assistance.
Advanced...
Remote Desktop
Allow users to connect remotely to your computer
Note: to further configure this terminal server, use Group Policy or the Terminal Services Configuration tool.
For more information about deploying, configuring, and administering this terminal server, see Terminal Server Help.
OK
Cancel
Apply

The users of the remote desk are the members of a Security Group in the Active Directory of the DNS. Access this group using the MMC console:

- Click on Start, click on Run, and in the text box, type mmc /s.
- Add the component Active Directory Users and Computers



- Select among the Security Groups the line named Remote Desktop Users in the Builtin directory.
- Right-click on Properties. This displays the group members:



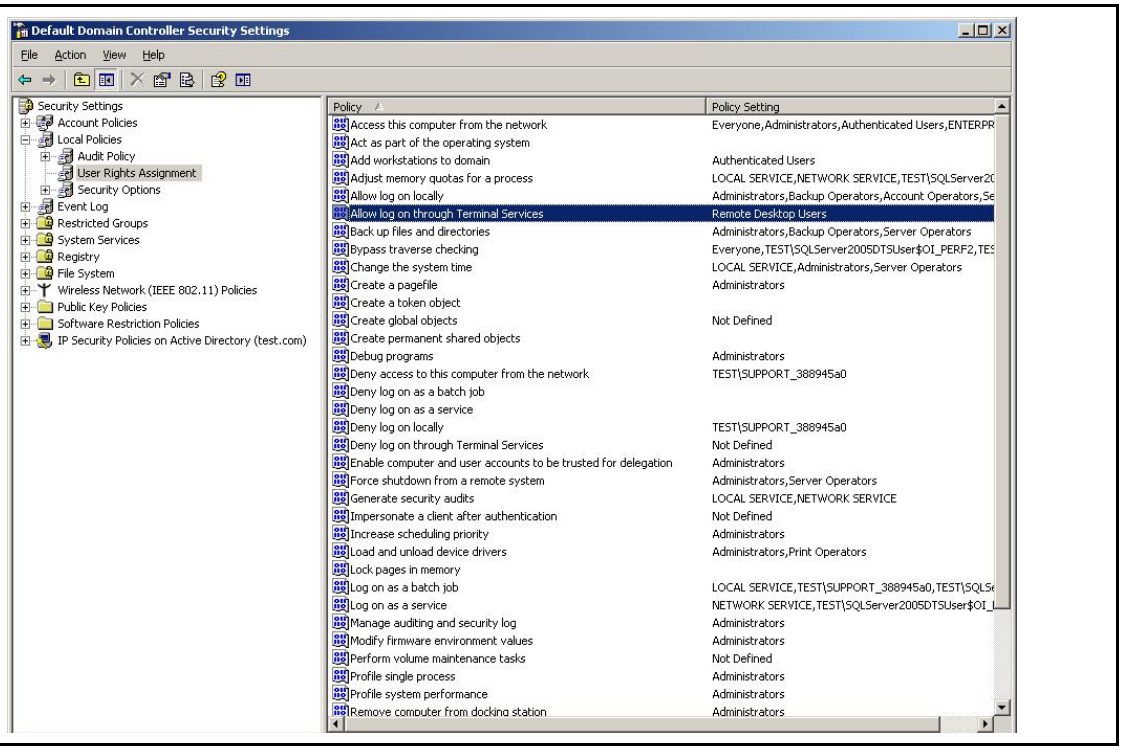
- Click on Add to add members entitled to remotely access the desktop. This is not valid if the server is a domain controller.

8.2.5 Connection to the Domain Controller in Administrator mode

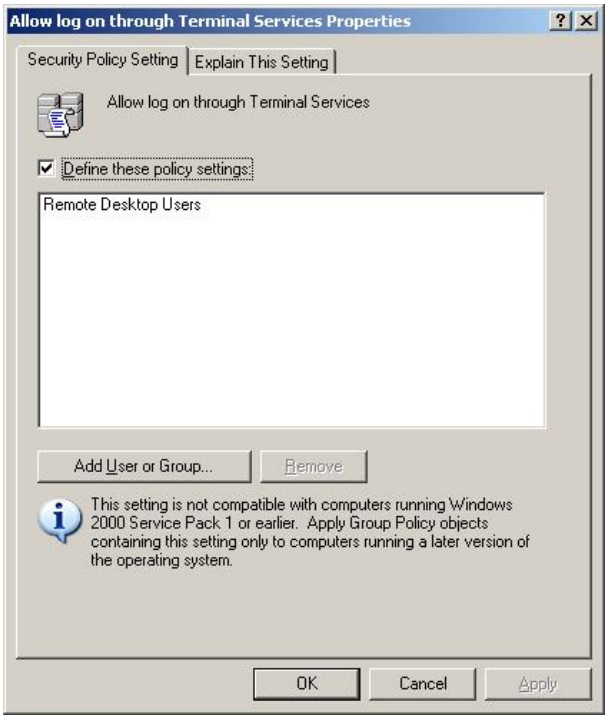
The domain controller has Active Directory installed.

It is indispensable to add the Remote desktop users group in the domain controller security policy. Open an Active Directory console as previously described.

- In the Default Domain Controllers Policy console, expand Computer Configuration; navigate to Windows Settings, then to Local Policies, and select User Rights Assignment:



To modify the default settings (Administrators, Remote Desktop users), double click on the line Allow log on through Terminal Services:

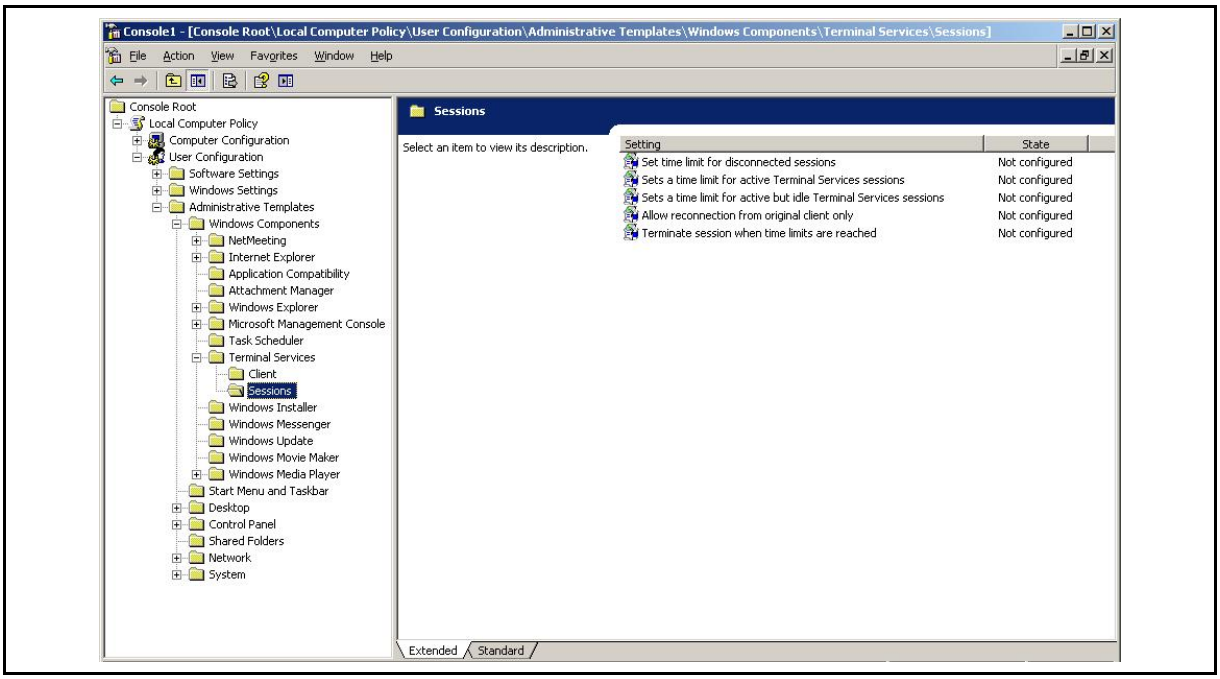

Allow log on through Terminal Services Properties
Security Policy Setting
Explain This Setting
Allow log on through Terminal Services
Define these policy settings:
Remote Desktop Users
Add User or Group...
Remove
This setting is not compatible with computers running Windows 2000 Service Pack 1 or earlier. Apply Group Policy objects containing this setting only to computers running a later version of the operating system.
OK
Cancel
Apply

This permits connections.

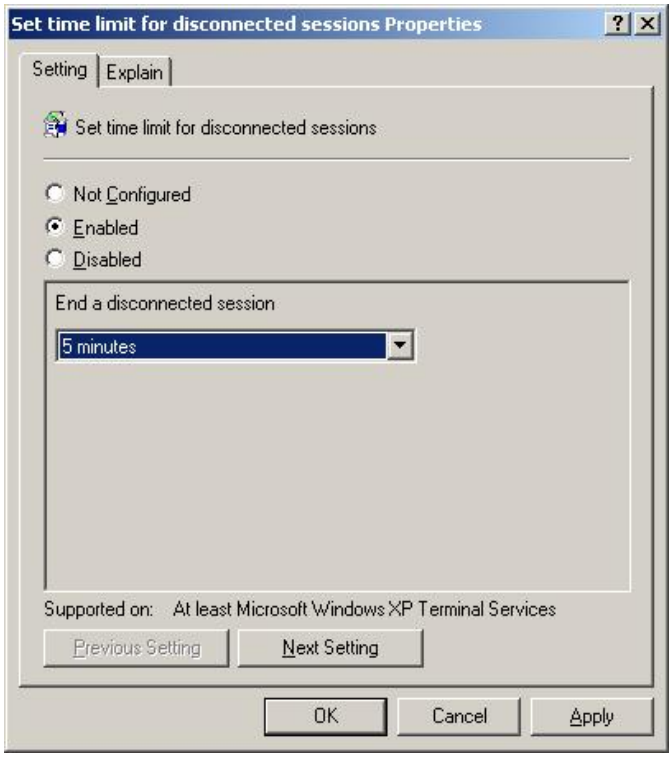
By default the members of the groups Users and Power Users are allowed to log onto the server locally. To remove these groups from those entitled, double click on the line Allow log on locally and choose Remove.

It is indispensable to modify the session opening time. For this:

- open an Active Directory console
- expand User Configuration and Administration templates; navigate to Terminal Server Services and select Sessions:



- Double click the line ‘Set time limit for disconnected sessions’ and modify the setting:



BLANK PAGE

FUNCTIONAL DESCRIPTION

CONTENTS

1.	**SCOPE OF THE DOCUMENT**	**3**
2.	**FUNCTIONAL DESCRIPTION**	**4**
2.1	**Control points**	**4**
2.1.1	Remote control points (RCP)	4
2.1.2	Substation Control Points (SCP)	4
2.1.3	Bay Control Points (BCP)	5
2.2	**Plant data interface**	**6**
2.2.1	Digital inputs	6
2.2.2	Digital measurements	6
2.2.3	Counters	6
2.2.4	Analogue inputs	6
2.2.5	Conventional Measurement CT/VT inputs	7
2.2.6	Conventional Protection CT/VT inputs	7
2.2.7	Digital outputs	7
2.2.8	Digital setpoints	7
2.2.9	IED Interface	7
2.3	**Process and apparatus data management**	**8**
2.3.1	Binary inputs (BI)	8
2.3.2	Measurement	10
2.3.3	Tap position indication processing	12
2.3.4	Metering	12
2.3.5	Energy counting	13
2.4	**Data logging and archiving**	**14**
2.4.1	Data logging	14
2.4.2	Data archiving	15
2.4.3	Reporting	16
2.5	**Control sequences**	**17**
2.5.1	Control sequence behaviour	17
2.5.2	Control sequence of switching devices	17
2.5.3	Close control of synchronised circuit breakers	18
2.5.4	Control sequence of transformers	18
2.5.5	Control of secondary devices	18
2.6	**Automatic control functions**	**19**
2.6.1	Interlocking	19
2.6.2	Configurable automations (PLC)	19
2.6.3	Fast configurable automation (PSL)	19
2.6.4	Built-in automatic functions	20

2.7 Alarms management 21
2.7.1 Types and definition 21
2.7.2 Alarm display 21
2.7.3 Alarm aknowledgement and clearing 21
2.8 IED management 22
2.9 Time management 23
2.10 System monitoring 24
2.10.1 Equipment operating modes 24
2.10.2 Equipment redundancy 24
2.10.3 Local/remote control operating modes 25
2.11 Engineering tools 26
2.11.1 System Configuration Editor (PACiS SCE) 26
2.11.2 Stand-alone Configuration Tool (SCT) 26
2.11.3 C264 Maintenance Tool (CMT) 27
2.11.4 Embedded Web maintenance server 27
2.12 PACiS Watch 28
2.12.1 Role 28
2.12.2 Use 28
2.13 Cybersecurity 31
2.13.1 General 31

3. PACIS ARCHITECTURES 32

4. PACIS ETHERNET NETWORK ARCHITECTURES 33

4.1 Simple star network 33
4.2 Redundant optical ring network 34
4.3 Dual Homing network 36
4.4 Virtual LAN 36

5. MULTI-LINGUAL SUPPORT 37

5.1 Italian Language 37
5.2 Greek Language 37

1. SCOPE OF THE DOCUMENT

This document is a chapter of the PACiS SYSTEM documentation. It is the functional description of PACiS SYSTEM and an overview of its elements.

2. FUNCTIONAL DESCRIPTION

2.1 Control points

2.1.1 Remote control points (RCP)

PACiS allows you to control a substation from remote control points (SCADA) generally located some kilometres away from the substation and usually able to control several substations.

PACiS can communicate simultaneously with different Remote Control Points (RCP) using separate communication protocols and separate databases.

PACiS can manage up to four RCPs and provides several SCADA interfaces corresponding to a wide range of communication protocols:

International standards:

- IEC60870-5-101
- IEC60870-5-104
- DNP 3.0

“de facto” standards:

- ModBus
- OPC
- CDC Type 2

Specific protocol:

- GI74
- CDC Type 2
- HNZ 66S15
- T101-SAS
- SAS

If needed other specific protocols can be taken into account and implemented.

Definition of number and types of communication protocols is user selectable using the PACiS System Configuration Editor (SCE).

2.1.2 Substation Control Points (SCP)

The whole substation can be controlled from one or several Operator Workstations usually situated inside the substation or in a communication room. This control is done via several dedicated Operator Interfaces (OI), running on PC-like computer (called the Operator Workstation), which provide to the user the following functions:

Control functions

- alarms acknowledgement and clearing
- control of switching devices (circuit breaker, switch, …)
- locking of switching devices
- control of transformers
- control of secondary devices
- control of internal automation

Maintenance functions

- full graphic representation of the system
- modify the settings
- system maintenance functions (databases)
- disturbance files upload
- monitoring analysing functions

Supervision functions

- access authorisation
- topological view of single line diagram
- full graphic representation of switching devices
- full graphic representation of analogue values
- full graphic representation of additional process information
- display of automations state
- display and modification of counters
- display of alarms in list form
- display of events
- display of states
- viewing of curves for archived or real-time analogue and digital data
- forcing, substitution, suppression of datapoints
- memo function
- discordance management
- hypertext online help
- reports creation
- hardcopy
- tooltips

NOTE: Depending on the different types of PACiS architectures, the system can exist in a configuration without any OI but with SCADA interface.

2.1.3 Bay Control Points (BCP)

At bay level, the control can be done via:

- a LCD Panel integrated to the MiCOM C264 which allows:
  - Displays of bay panels, events, measurements, alarms,…)
  - Control of devices, alarm acknowledgement,…)
- push buttons or remote contacts (electrically wired) which allows mainly to display and control the switchgear and transformers.

2.2 Plant data interface

2.2.1 Digital inputs

Digital inputs (DI) are binary information related to the presence or to the absence of an external signal, delivered by a voltage source. The input nominal voltage Un can take one of the following DC values according to IEC 38: 24 Vdc, 48 Vdc, 60 Vdc , 110 Vdc, 125 Vdc, 220 Vdc.

The DI is equal to 1 if the signal is present and is equal to 0 if it is absent. The signal polarity can be positive or negative. The configuration allows if necessary to invert the DI value by software.

The acquisition period of digital inputs is fixed and is equal to 1 ms in MiCOM C264 computers range. Debouncing and stability filtering is applied in order to confirm the change of state of a digital input.

Every change of state is time tagged as soon as it has been detected.

2.2.2 Digital measurements

PACiS computes digital measurements issued from wired inputs (up to 64) associated to the following different encodings: BCD, Binary, Gray code, 1-among-N, decimal

Digital measurements are read according to a user-selectable cycle and are filtered (multiple scan process).

A digital measurement is invalid in case of incoherency between the type of encoding and the number of bits set to 1 (exemple: more than one bit is set in a 1-among-N encoding)

2.2.3 Counters

The energy metering devices deliver pulses corresponding to a calibrated quantity of energy. Each valid pulse increments the value of an accumulator used to compute the quantity of energy delivered during a given period.

Counters are acquired on the same boards as the digital inputs and may be single (one contact) or double counter (two contacts, the true contact “TC”, and the complemented contact “CC”).

For a single counter (SCT) the value of the accumulator is incremented after a low to high transition, confirmed after a filtering time. Up to 24 SCT can be acquired on a per MiCOM C264 computer basis.

For a double counter (DCT) pulses are detected in the same manner as for SCT, on the TC (True contact) variations. The pulse CC (the complemented contact) must be inverted regarding the TC contact.

The maximum frequency of the pulse is 20 Hz.

2.2.4 Analogue inputs

Analogue inputs (AI) are voltage or current DC signals delivered by transducers, and representing an external value.

Input ranges are:

- For voltage: ± 10 V, ± 5 V, ± 2.5 V, ± 1.25 V
- For current: 0 - 1 mA, 0 - 5 mA, 0 - 10 mA, 0 - 20 mA, ±1mA, ±2,5 mA, ±5 mA, ±10 mA, ±20 mA, 4 - 20 mA

The analogue inputs are acquired on a periodical basis. There exist two acquisition cycles:

- a short cycle (N_{sc} x 100ms, N_{sc} configurable from 1 to 10 with a default value of 1)
- a long cycle (Nlc x 500ms, Nlc configurable from 1 to 20, with a default value of 2)

The accuracy of the complete acquisition chain is 0.1 % of the full scale for each range at a reference temperature of 25 °C.

The Analogue to Digital Converter has a 16-bit resolution (15 bits + sign bit) and the zero offset value is computed by the conversion of a 0 V voltage reference. An AI is time stamped with the date/time of the scanned value.

2.2.5 Conventional Measurement CT/VT inputs

Measurement CT´s and VT´s are available at a 50 Hz or 60 Hz nominal frequency (f_{nom}).

They are acquired via a dedicated CT/VT board (TMU 200 or TMU 220) embedded in the MiCOM C264.

2.2.6 Conventional Protection CT/VT inputs

ProtectionCT´s and VT´s are available at a 50 Hz or 60 Hz nominal frequency (f_{nom}).

They are acquired via a dedicated CT/VT board (TMU 210) embedded in the MiCOM C264P.

2.2.7 Digital outputs

Digital outputs are used to apply a switching voltage to an external device in order to execute single or dual, transient or permanent commands. The applied voltage is fed from an external power supply.

The external voltage is connected to the controlled device by a relay, thus isolating the logic part of the board from the external power supply. The relays can be single pole (one contact) or double pole (two contacts) N/O relays. There are also inverter relays (N/C) with one normally open and one normally closed contact, which can be used when positive security is required.

2.2.8 Digital setpoints

A Digital Setpoint is a set of several digital outputs (up to 48), each one of them representing a bit of its value. Digital Setpoints are used to send instruction values to the process or to auxiliary devices.

The Digital Setpoints are processed on the same boards as the Digital Outputs. The Digital Outputs characteristics described here above apply on Digital Setpoints.

Digital Setpoints can be encoded with BCD, Binary, Gray, Decimal, 1 among N codes.

Moreover a supplementary binary output can be used for the sign bit and a dedicated binary output can be used to enable or not the reading of the value by the external device.

2.2.9 IED Interface

The IED Interface is used for a line-to-line or multipoint interconnection between the different system devices. The data transfer takes place with different specific serial protocols.

The provided interfaces are EIA RS-232 transmission, EIA RS-485 transmission, Fibre optic transmission

2.3 Process and apparatus data management

2.3.1 Binary inputs (BI)

PACiS system manages five types of binary inputs:

- Single Point (SP) derived from one Digital input
- Double Point (DP) derived from two Digital inputs
- Multiple Point (MP) derived from N Digital inputs (up to 16 in case of states, up to 64 for TPI)
- System Input (SI) information related to the system, to configurable and built-in automations or to electrical process but without acquisition possibilities
- Group: logical combination of BI

SP, DP and MP are acquired via digital input boards or via IEDs connected by a serial link. SI and Groups are generated by the computer application layer.

2.3.1.1 Single, double and multiply points processing

The following table shows filterings applied to digital input according to its type.

	SP input	DP input	MP input
Toggling filtering (1)	X	X	X
Persistence filtering (2)	X	X	
Motion filtering (3)		X	
Undefined state filtering (4)			X

1. Toggling filtering: applied in order to eliminate toggling transitions.
2. Persistence filtering: DI must stay in the same state on a certain period of time T otherwise are not taken into account.
3. Motion filtering is applied to double points in order to avoid take into account transient states: (00, 11).
4. Undefined states of Multiple Points are filtered in order to avoid to take into account transient states: all DI in the SET state, all DI in RESET state, or more than one are in the SET state.

Toggling parameters, persistence time, motion and MP filtering time are configurable.

No filtering (except persistence one) is applied to SI and Groups inputs.

Binary inputs can be manually suppressed (they are not processed until unsuppression), or substituted by another state. When a binary input becomes invalid, the operator can force it by a valid state. The binary input is automatically unforced when it becomes valid again. The configuration allows also the user to define automatic forcing when a binary input becomes invalid.

Binary resulting states after processing

	Single Point	**Double Point**	**Multiply Point**
CONFIRMED STATES	RESET SET	OPEN CLOSE	STATE1 to STATE32
MOTION FILTERING/ MP FILTERING		JAMMED UNDEFINED	UNDEFINED
TOGGLE FILTERING	TOGGLING	TOGGLING	TOGGLING
SELF CHECK FAILURE	SELFCHECK FAULTY	SELFCHECK FAULTY	SELFCHECK FAULTY
LOSS OF COMMUNICATION	UNKNOWN	UNKNOWN	UNKNOWN
SUPPRESSED BY OPERATOR	SUPPRESSED	SUPPRESSED	SUPPRESSED
SUBSTITUTED BY OPERATOR	SUBSTITUTED RESET SUBSTITUTED SET	SUBSTITUTED JAMMED SUBSTITUTED OPEN SUBSTITUTED CLOSED	SUBSTITUTED STATE 1 to 32
FORCED BY OPERATOR/ AUTOMATICALLY	FORCED RESET FORCED SET	FORCED JAMMED FORCED OPEN FORCED CLOSED	FORCED STATE 1 to 32

2.3.1.2 System Inputs (SI)

System inputs are binary information related to:

- an equipment or system internal state, such as hardware faults or system faults.
- configurable or built-in automation (status of the automation, binary input created by the automation, …).
- electrical process information which have no acquisition possibilities (i.e. no acquisition through DI or through serial communication) but which must be managed by the MiCOM C264: the status of these information are saved in non-volatile memory.

A SI is of SP, DP or MP type and can belong to any type of group. The processing of a SI is the same as the SP / DP / MP but there is no motion filtering nor MP filtering on SI.

2.3.1.3 IED Inputs

These inputs are acquired from IEDs or protective relays via the station bus or legacy bus.

An IED input is of SP, DP or MP type and is processed as described above.

2.3.1.4 Groups

A group is a logical OR or AND or NOR or NAND combination of binary inputs described above or other groups.

A group is processed as a SP and so can take the following states: Set, Reset, Invalid, Suppressed. A group can be manually or automatically suppressed, forced or substituted.

A group is time stamped with the date/time of the last datapoint which has modified the group status.

2.3.1.5 Binary inputs transmission

The Binary Inputs are transmitted on a client-server basis on the Station Bus (IEC61850). A BI can be transmitted using two modes:

- **Report based mode**: a BI can be configured to be transmitted in Report mode. In this mode, a confirmed change of status is spontaneously transmitted to the subscribers with the time stamping and the reason for change.
- **GOOSE based mode**: in this mode, the change of status is transmitted in multicast to the configured receivers. Only the BI unfiltered states with their time stamping are transmitted, the reason for change is not.

Basically, the Report mode is used to transmit filtered data for displaying, printing and archiving. The GOOSE mode is used to transmit data as soon as possible after their acquisition and as quickly as possible, for automation purpose.

During a loss of communication between a client and a server, the different information are buffered at MiCOM C264 using the standard IEC61850 concept and after the communication reconnection, they are transfert to the different clients to update their repective functions.

2.3.2 Measurement

A measurement can be acquired by using:

- an analogue input
- a digital measurement
- a serial communication link with an IED
- a CT/VT input

2.3.2.1 Measurement processing

Configuration process allows the user to define for each measurement a scaling law (linear, quadratic) and up to 6 thresholds for which the detection caused by a measurement variation can create an event and alarm.

Moreover, for 4-20 mA transducers, a special feature is implemented to avoid fleeting values around 4 mA.

Measurements can be manually suppressed (they are not processed until unsupression), or substituted by another value. When a measurement becomes invalid, the operator can force it by a valid value. The measurement is automatically unforced when it becomes valid again. The configuration allows also to the user to define automatic forcing when a measurement becomes invalid.

Measurement resulting states

State	**Comment**
VALID	Not in one of the below states
SELFCHECK FAULTY	Detected “faulty” by the acquisition component
SUBSTITUTED	By operator
FORCED	By operator / Automatically
SUPPRESSED	By operator
UNKNOWN	Loss communication.
SATURATED	Detected “saturated” by the acquisition component
UNDEFINED	Scaling management
OPEN CIRCUIT	Open Circuit Management
OVERSHOOT[1..3]	Threshold management
UNDERSHOOT[1..3]	Threshold management

2.3.2.2 Measurements Transmission

The measurements are transmitted on a client-server basis on the Station Bus network by using two modes:

- **Report based mode**: the measurement is transmitted to the subscribers with its value, its status, its time stamping and the reason for change
- **GOOSE based mode**: the measurement is transmitted in multicast to the configured receivers.

Measurements can be transmitted:

- **cyclically** with a short period from 0 to 60 seconds (step 0,1 second) or a long period, from 0 to 60 seconds (step 0,5 second). Periods are user selectable.
- **on variation:**
  - **according to a % of the full scale value:** the value is sent if the acquired value is different of more than the specified delta from the full scale value (variation is user selectable)
  - **according to a % of the current value:** the value is sent if the acquired value is different of more than the specified delta from the previously transmitted value (variation is user selectable)
- **on Threshold violation**: if an overshoot or an undershoot occurs, the measurement is transmitted. The measurement is also transmitted at the end of an overshoot or at the end of an under shoot, for example threshold minus hysteresis (thresholds and hysteresis are user selectable)
- **upon trigger**: upon change of state of a SP, a DP or a SI, one measurement or a group of measurements are transmitted. (the association Measurements and SP, DP, SI are user selectable)
- **on Change of state:** measurements are always transmitted when the change state (VALID, AKNOWN, SUBSTITUTED,…)

2.3.2.3 CT/VT Calculations

The following measurement values are provided using the CT/VT inputs acquisition (TMU 200 or TMU 220):

- RMS currents and voltages
- Frequency (with a 0,01 Hz precision)
- Active power P (Watts – total and on a per phase basis – with a 0,5% precision)
- Reactive power Q (Vars – total and on a per phase basis)
- Apparent power S (VA – total and on a per phase basis)
- Power factor pf (total and on a per phase basis) – pf = P / S
- Sequence components (Id=>I1, Ii=>I2, Vd=>V1, Vi=>V2 (match Px40 or pos/neg to match Px30))
- Phase angles (with a 1° precision)
- Total Harmonic Distortion (THD) & Total Demand Distortion (TDD) – Harmonics are evaluated up to the 15^{th} order.
- Magnitudes
- Synchrocheck information: ΔF, ΔV, $\Delta\varphi$

2.3.3 Tap position indication processing

The tap position indication (TPI) can be acquired on:

- digital input boards. It could be:
  - a multiple point (MP)
  - a digital measurement (Decimal, Gray, BCD)
- analogue inputs (by measuring a current): a minimum value Imin (mA) corresponds to the lowest position (1) of the tap , and a maximum value Imax corresponds to the highest one.
- TPI can be suppressed, substituted and forced like digital inputs and measurements.

2.3.3.1 TPI resulting states after processing

State	**Comment**
VALID	Not in one of the below states
SELFCHECK FAULTY	Due to an AI board fault or a DI board fault
SUBSTITUTED	By an operator
FORCED	By an operator
SUPPRESSED	By an operator / automatically
UNKNOWN	If the tap position is acquired via a transmission link, the information is unknown when the link is disconnected.
UNDEFINED	Due to a wrong encoding for a digital acquisition, or a saturation, an open-circuit or an out-of-range value for an analogue acquisition
OVERSHOOT[1..3]	there exist 3 “Overshoot” states, one for each upper threshold violation. Only one could be set at one time
UNDERSHOOT[1..3]	there exist 3 “Undershoot” states, one for each lower threshold violation. Only one could be set at one time

2.3.3.2 TPI transmission

The TPI are transmitted on a client-server basis on the Station Bus network using the same mechanisms than the measurements. They are transmitted as soon as a value change or a status change is detected.

2.3.4 Metering

Metering values (non-tariff metering) are issued from single and double counters. They represent the number of pulses taken into account (32-bit values).

Digital counter acquisition is stored to accumulators in non-volatile memory. The accumulator is incremented at each valid counter pulse.

IEDs Counters transmitted cyclically are stored to the periodic register and FIFO memory.

An operator can force the metering values. The modification could be a reset of the counter.

2.3.4.1 Counter resulting states after processing

State	Comment
VALID	not in one of the below states
SELFCHECK FAULTY	Due to the SELFCHECK FAULTY of the DI
UNKNOWN	If the counter is acquired via a transmission link, the information is unknown when the link is disconnected.
UNDEFINED	Due to a counting failure of DCT (non-complementarity of the two contacts)
OVERRANGE	when the maximum value is reached

2.3.4.2 Counters Transmission

The counters are transmitted on a client-server basis on the Station Bus network using the same mechanisms than the measurements

2.3.5 Energy counting

The energy counting function aims to calculate exported and imported active energy (in kWh) and exported and imported reactive energy (in kVarh) from active and reactive power issued from CT/VT calculation.

The energy values are transmitted on a client-server basis on the Station Bus using same mechanisms than the counters.

2.4 Data logging and archiving

2.4.1 Data logging

The Data Logging function is the logging of PACiS information on printers. Three types of printers are available:

- the SOE printers (Sequence Of Event)
- the LB printers (Log Book)
- the HC printers (Hard-Copy)

PACiS manages:

- a maximum of 2 redundant SOE printers (i.e. 4 SOE printers) and 2 redundant LB printers (i.e. 4 LB printers) at a system level, managed by the OI. These printers can be serial or network ones.
- a maximum of 1 LB printer at a computer level (serial printer)

2.4.1.1 Sequence Of Event (SOE) printer

SOE printer is a dedicated printer for printing only SP, DP and MP events attached to the primary process only.

The 7 following BI properties can be printed. The position of each property in the printed line (i.e. position 1, 2, 3, 4, 5, 6 or 7) is defined in configuration:

- Chronology
- TimeStamp and synchronisation status (the synchronised / not synchronised)
- Origin: substation name, voltage level name, bay name, module name
- ObjectName: BI name
- ObjectMessage: BI resulting state.
- Origin Category: specifies the category of the originator that caused the change of value (bay-control, station-control, remote-control, automatic-bay, automatic-station, automatic-remote, maintenance, process)
- Origin Identification: name of the originator who caused the change of value.

NOTE: For the following Common Data Classes these two last columns are empty:

- SPS (Single Point Status)
- DPS (Double Point Status)
- INS (Integer Status)
- ACT (Protection Activation information)
- BCR (Binary Counters)
- MV / CMV / WYE (Measurement values, Complex measurements, Harmonic values)

2.4.1.2 Log Book (LB) printer

Types of events printed on the LB printer can be:

- Binary inputs (SP, DP, MP, SI and Groups)
- Tap position indication
- Measurement
- Operator action (Log-in and log-off, Devices control)
- Alarm acknowledgement / clearing

One or several types of events can be printed: the choice is made by configuration. The selection of the LB printer destination (1, 2, or both, for printer at system level) is made by configuration on a per data basis.

The list of event states (for BI, Tap Position Indication and measurements) which will be printed can be defined in configuration. A printed information will be also archived.

Properties printed are the same than SOE printers above.

2.4.1.3 Hard-copy printer

Hard-copy printers allow printing “hardcopy” views of the Operator Workstation and printing of reports

2.4.2 Data archiving

The Data Archiving function is the historisation of PACiS information:

- at computer level: local archiving
- at OI level: central archiving

2.4.2.1 Local archiving

Local archives are implemented at the level of the equipment that acquires or process the information (i.e. the MiCOM C264s). Events are stored in non-volatile memory.

The number of events recorded into a local archive depends on the type of equipment.

The archived events can be viewed on the computer local HMI.

Events

The data archiving of events is configurable on a per event basis. The following events can be archived:

- changes of state of binary inputs (SP, DP, MP, SI, Groups)
- changes of state of measurements
- changes of state and value of Tap Position Indications
- devices Control actions and acknowledgements

The archived events can be viewed on the computer local HMI.

Fast Waveform Recording

Fast Waveform recording allows to store samples at the maximum sampling frequency.

Waveform records are stored using COMTRADE 2001 binary format.

Slow Waveform Recording

Slow Waveform recording allows to store measurements on a long period.

Waveform records are stored using COMTRADE 2001 binary format.

2.4.2.2 Central archiving

Events central archiving

PACiS allows to have central archives on the hard-disk of the Operator Workstation, using a SQL Server database.

Measurements central archiving

The measures and associated mean values are archived in the central SQL server database, as the events in the following tables:

- Daily table for the mean values of the day. These tables are stored during 35 days.
- Monthly table for the minimum, maximum, mean values, computed at a reference time (configurable) of a day. Monthly tables are stored during 15 months.
- Yearly table for the minimum, maximum, mean values, computed at a reference time (configurable) of a month. Yearly tables are stored during 5 years.

Backup central archiving

A backup of the central archive (i.e. of the SQL database) is allowed at a configured date / time

Waveform and Disturbance Files

These files, generated at a local level, can be automatically uploaded from a device. Only one central file archiving is defined in the system. The automatic upload could be activated / de-activated by the operator. The disturbance files are stored in COMTRADE 2001 binary format.

A storage policy is defined to avoid filling up the hard disk:

- a maximum of 10 files can be stored on a per device basis: the oldest is automatically removed when a new one is uploaded
- this principle defines a storage area per system database version
- global disk space of storage area is defined in local setting

2.4.3 Reporting

PACiS provide a mechanism for creating reports showing:

- real-time information
- information collected by central archiving function

2.5 Control sequences

2.5.1 Control sequence behaviour

The control sequences can be initiated from any control point (RCP, SCP, BCP and DCP).

By configuration a control may be executed to one of the following modes:

"**Select Before Operate once**" mode (**SBO once**): usually for circuits breakers and disconnect switches. The device must be selected before allowing the execution. In that case the device is managed in two phases: selection and execution. Device unselection is done automatically by the computer.

"**Select Before Operate many**" mode (**SBO many**): usually for tap positioning of transformers. The device must be selected before executing one or more controls before reaching the expected position (low/raise). In that case the device is managed in two phases: selection and execution. The execution phase is repeated for every new control. The deselection of the device must be done by the initiator of the request.

"**Direct Execute**" mode: usually for ancillary devices a control may be performed directly without need selection (**DE**).

Control sequences are executed if the computer is in "operational" mode. However PACiS system allows to perform control sequences in "test" mode in order to simulate controls for devices. In this mode output relays are not activated, controls are not sent to IEDs or on station bus, and only the control acknowledge is managed. Some system outputs controls such as "switch database", "change computer mode" are allowed in maintenance mode.

The following checks (user-selectable) can be performed before the acceptance of the control:

- the Inter-control delay has expired (time between two sequence in the same device)
- substation, bay and SBMC mode allow the control
- interlock equation and topological interlocking allow the control
- no automation is running for the device
- the device is not locked
- the current status of the device is on the opposite state
- uniqueness control: only one control at a time for the device

If these checks are configured, they are checked by the MiCOM C264 in each phase of the control sequence (allowing the switching devices to operate in security).

An acknowledgement (positive or negative) can be issued, sent to the different control points, archived and printed.

"Interlocks" can be by-passed by the operator, depending on its access rights.

The operator request is also printed and archived.

2.5.2 Control sequence of switching devices

PACiS control switching devices such as circuit breaker, disconnector or earth switch. They are managed in "Direct execute" or "SBO once" mode.

The allowed controls are open and close commands. Moreover the "close/open" control the device may have, by configuration, a "selection" output control. In this case the device is managed in "SBO once" mode. The device is selected in the selection phase.

2.5.3 Close control of synchronised circuit breakers

Synchronised circuit breakers may have specific features. These features ere user-selectable and are taken in account by the control sequence upon a close request:

- the device is controlled by an external synchrocheck module or internal automatic function
- the synchrocheck module (internal or external) is setting on/off manually or automatically

Moreover, during waiting the closing of the device by the synchrocheck module the initiator of the request may:

- cancel the request
- close the device by forcing request

2.5.4 Control sequence of transformers

PACiS control transformers by dealing with associated tap changer positions.

The allowed controls are « raise » command (current tap position+1) and « lower » command (current tap position-1).

Additionally of the common checks of control sequence the computer proceeds to the following verifications:

- only raise command is allowed if the tap position value is the smallest one authorised
- only lower command is allowed if the tap position value is the higher one authorised

Transformers can be managed in the three modes (Direct Execute, SBO once and SBO many):

- **Direct Execute**: only one control raise or low is performed in the control sequence. The initiator of the request must perform many “Direct Execute” sequences before reach the expected position.
- **SBO once**: the sequence is similar to the “Direct Execute” but the execution phase is preceded by a selection phase. In this phase are performed all controls checks and the selection of the device (if it is configured).
- **SBO many:** after the selection phase, many controls raise or low can be performed in the same sequence in order to reach the expected position. The sequence ends only after an unselect request from the initiator.

2.5.5 Control of secondary devices

PACiS control secondary devices like protective relays or IED allowing to (non-exhaustive list):

- Modify the setting groups parameters used by a protection equipment (for example 1 among N command type if N setting groups are available for the protection)
- Reset some internal indication (for example single command type to reset alarm indication on a protective relay)
- Set active or inactive an external equipment or apparatus (for example ON/OFF or IN/OUT single or double command type)
- Send analogue or digital Setpoints to external apparatus or equipment
- De-active the alarm klaxon
- Control the substation / room lights

2.6 Automatic control functions

2.6.1 Interlocking

Interlocking function provides authorisation to control a HV or MV switching device (circuit breaker, disconnector, earthing switch), protective devices and auxiliary equipment from any control point (RCP, SCP, BCP, DCP, automation).

Interlocking equations are written using logical equations of all process information. The interlocking equation does not only use the value of the information but also the validity of the information.

The configuration process allows the user to define or not for each transition (open/close) an interlocking equation.

Each MiCOM C264 manages the interlocking equations of its own switching devices.

2.6.2 Configurable automations (PLC)

PACiS allows the user to configure specific control sequences or automations (for example switching sequences, busbar transfer, load shedding, GIS-pressure, etc …) during the configuration phase. The language used (PLC-program) takes into account the IEC 61131-3 standard.

The execution of the automation sequences is cyclic: nevertheless, a dedicated mechanism is provided to avoid data lost. Maximum number of cyclic PLC-programs is 32.

Each PLC-program runs on one computer, which means a PLC-program cannot be distributed within the system. However, it is possible to use information obtained by other computers.

Automations can be triggered:

- by operator request
- by events (digital or analogue input state changes)
- other automation request

PACiS embeds the ISAGRAF™ tool (provided by ICS Triplex company) to perform the PLC

2.6.3 Fast configurable automation (PSL)

Due to the range of PLC cycle time (no less than 50 ms), another type of fast automation is provided in PACiS: the Programmable Scheme Logic automations.

These automations are event-driven: they are calculated each time an input changes (i.e. there is no cycle time). Inputs can be BI and measurements.

PSL are logical equations that use the following functions:

- AND, OR, XOR, NOT, NAND, NOR operators
- “bistable” function
- pickup and drop-off timers (from 10 ms to 60 seconds, by step of 10 ms)
- BI setting – the system BI is:
  - SET if the PSL is TRUE
  - RESET if the PSL is FALSE
  - INVALID if the PSL is INVALID
- Digital Output setting – the DO is:
  - closed if the PSL is TRUE
  - opened if the PSL is FALSE or INVALID (only in case of permanent DO)

2.6.4 Built-in automatic functions

PACiS performs a wide range of automatic functions for the substation control activity.

These functions can be activated, by-passed, deactivated (and re-activated) by authorised operators.

2.6.4.1 The Automatic Voltage Regulation

The Automatic Voltage Regulation (AVR) function is used to automatically maintain the correct voltage at the lower voltage of transformers. Secondary voltage is changed by controlling the tap changer of transformers.

2.6.4.2 Synchrocheck

The PACiS synchrocheck function is designed to measure two voltages with respect to phase angle, frequency and magnitude to safeguard against the interconnection of two unsynchronised systems. The voltage measures come from VT's. Up to two circuit breakers can be managed with the same computer synchrocheck.

Phase-to-phase Synchrocheck with the TMU210

Phase-to-phase synchrocheck allows you to configure a synchrocheck function with a delta wiring. Do this configuration at the TMU210 level and use the attributes "type of connection" and "reference phase".

2.6.4.3 Auto-Recloser

PACiS provides a built-in auto-recloser function for transient or permanent fault elimination. Auto-reclosing cycles and temporisation cycles can be defined during configuration process.

2.6.4.4 Pole discrepancy protection

PACiS provides a built-in pole discrepancy protection to allow circuit breaker trip in case of pole discrepancy.

2.6.4.5 Trip Circuit Supervision

The Trip Circuit Supervision function allows to raise an alarm into PACiS if a circuit breaker is still closed after a relay trip order.

The MiCOM C264 are able to support the 2 diagrams used in Trip Circuit Supervision:

- Trip Circuit Supervision with one Digital Input + external resistor.
- Trip Circuit Supervision with two Digital Inputs without external resistor.

2.7 Alarms management

2.7.1 Types and definition

Alarms can be generated by a change of state of a digital point, a measurement threshold violation, a PACiS internal fault (for example: loss of communication, computer faulty).

Digital points and measurements involved in alarms management can be issued from wired inputs or from IED or protective relays or from PACiS internal computation (for example digital groups).

Alarms can be defined as immediate or differed (with an associated user-selectable delay) and can have an associated audible alarm. The audible alarm can also be immediate or differed.

Alarms can be associated to each state of event (open, close, jammed,..) or to a measurement threshold (in case of violation) and may have a different gravity level (0..5).

Four types of alarm management are available on PACiS system and are user-selectable during configuration process:

- « state basis » alarm management: one alarm for each state is displayed
- « gravity level basis » alarm management: only one alarm for each gravity level is displayed. The previous one is replaced by the current one with same gravity level
- « data basis » alarm management: only the last alarm is displayed. The previous one is replaced by the current one
- “Spurious alarms” management: are defined for events which appear but never disappear (control acknowledgement for example)

Only the “data based” alarm processing is managed by the MiCOM C264 .

2.7.2 Alarm display

SCP level: the alarms are displayed via the HMI at SCP level, using:

- dedicated windows displaying:
  - the chronologically sorted list of the alarms (with additional sorting criteria as geographic or functional)
  - the last N alarms (N being user-selectable during configuration phase)
  - with different colours for each line of the previous lists, depending on the alarm state
- graphic pictures defined during configuration phase, displayed in the different views, which can be associated to the presence and the states of alarms for a device, for a bay, for a voltage area, for the whole substation, etc.

BCP level: the alarms are displayed in the form of one list in the panel. This list is a circular queue and is displayed in a scrollable view.

2.7.3 Alarm aknowledgement and clearing

An alarm can be acknowledged by an operator, to signify that it has been taken into account. Acknowledgement can be done by the operator at SCP or BCP level. An acknowledgement done at BCP level has no impact at SCP level and vice-versa.

Independently of the alarm acknowledgement, the audible annunciation can be acknowledged by an operator or automatically after a user-selectable delay

An alarm can be cleared only if the reason of its apparition disappear (becomes inactive) and was acknowledged by an operator.

An alarm can also be configured as « to be cleared automatically » when it becomes inactive and is acknowledged.

2.8 IED management

A wide range of IED can be fully integrated into PACiS via connection to different types of legacy busses or IEC61850 protocol.

Implemented protocols:

- IEC61850 on station bus
- IEC 60870-5-101 on legacy bus
- IEC 60870-5-103 on legacy bus
- Modbus on legacy bus
- DNP 3.0 (level 2) on legacy bus

These protocols are fully implemented in PACiS.

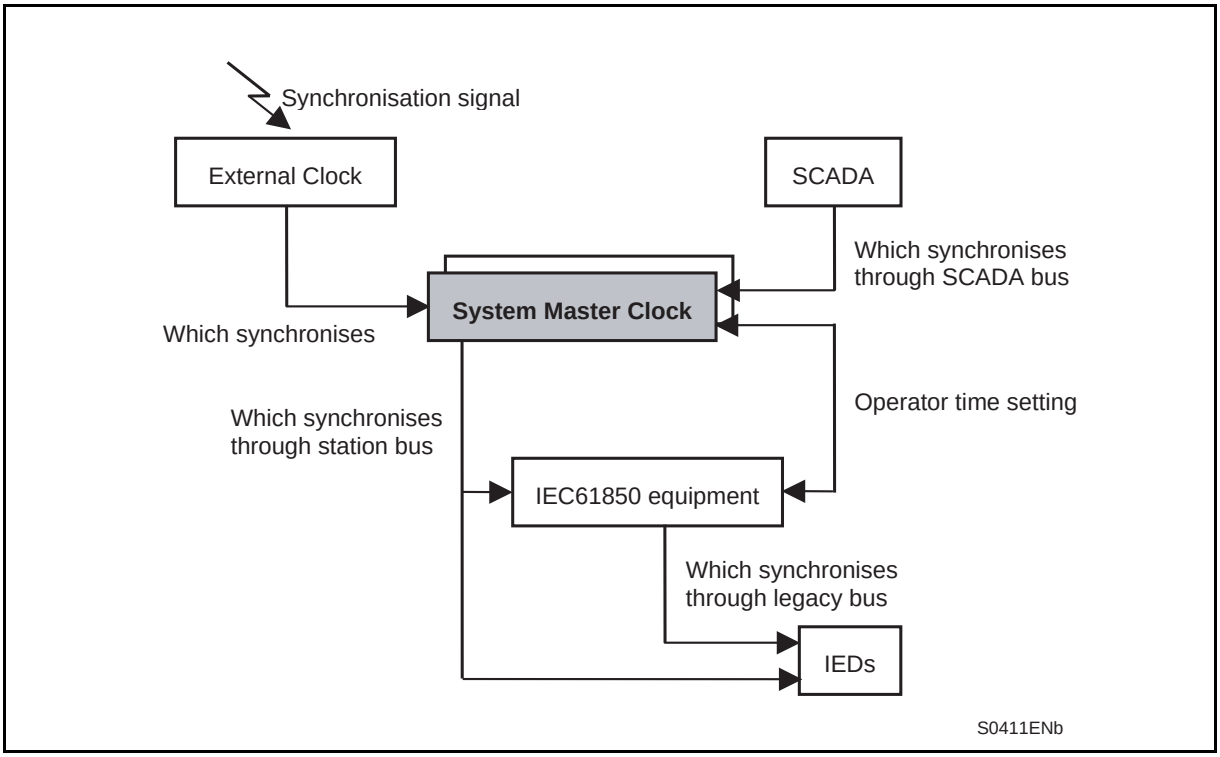
Third party protocols will be implemented using external converter over legacy bus protocols or station bus protocol.

2.9 Time management

PACiS system provides a time synchronisation mechanism, which allows the connected devices to have the same date/time. This synchronisation allows particularly the time tagging of events, the synchronising of the reports and programmed actions at source.

In a PACiS system, the external clock is connected to one MiCOM C264 (or two in case of computer redundancy) which is the “System Master Clock”.

The System Master Clock equipment is considered as the unique date/time reference for the whole system. It is connected on the Station Bus and it re-distributes the date/time reference to the other PACiS components (MiCOM C264, IEDs). The equipments connected on the Station Bus can communicate with IEDs connected on Legacy Bus. In this case, they synchronise their IEDs through the legacy protocols.



In the event that the external clock does not exist or is lost, the System Master Clock equipment can be synchronised by a SCADA or by an operator. Synchronisation priority of the System Master Clock is in the following order:

1. From the external clock (if it exists)
2. From the SCADA (if it exists) in case of failure of the External Clock (only if the SCADA protocol is managed by the System Master Clock computer)
3. From the operator in case of failure of the External Clock and the SCADA

Each Station Bus equipment after reception of a synchronisation message performs its local update procedure:

- MiCOM C264: if the delta between the local clock and the synchronisation message is less than 20 ms, a “smooth” increase/decrease of the local clock is done. Otherwise, the local clock is immediately set with the date/time of the synchronisation.
- PC local clock is updated using the operating system procedures.

PACiS system is capable to deal automatically with seasonal time changes by using indications coming from the external clock or using the Time Zone table.

In case of lost synchronisation to one of the different equipment (master clock equipment, Station Bus equipment, legacy equipment) is signalled (printed archived, alarmed).

2.10 System monitoring

2.10.1 Equipment operating modes

PACiS system equipments (MiCOM C264, PACiS GTW, PACiS OI server) may work in one of the following operating modes:

- **Operational**: the equipment is working correctly (all the functions are executed)
- **Test**: all functions are executed except activation of the relays of local output controls. The equipment simulates a positive acknowledgement for control sequences simulation. Note the output controls continue to be sends to the IEDs or to other computers.
- **Maintenance**: the equipment is working but only some functions are executed, generally the “supervision functions” (download and display data base information, communications state,…).This mode is requested by the operator or reached automatically in case of data base incoherence.
- **Faulty** (only for MiCOM C264): the equipment is working but only some functions are executed, generally the “supervision functions “, functions not involved in the management of the electrical process. This mode is a consequence of a failure detected on the equipment.
- **Initialisation** (boot): transitory mode between equipment power-up and Operational, Maintenance or Faulty mode
- **Halt**: the equipment is out of service due to detection of fatal error

The Operating mode can be changed locally (at equipment level) or from Operator workstation.

2.10.2 Equipment redundancy

2.10.2.1 PACiS OI twin server redundancy

More than one PACiS OI can be present inside the substation allowing operators:

- to control the substation from some different places
- to continue to control the substation from SCP level if a single failure occurs involving one PACiS OI

Two types of redundancy are available:

- server redundancy: the OI servers are redundant, allowing redundancy of alarms, events and historian functions. An OI client will switch from a server to the other one after a delayed failure detection.
- client redundancy: up to eight OI clients can be configured, allowing multiple points of control for the operator

NOTE: Printers attached to PACiS OI can be redundant

2.10.2.2 Station Bus redundancy

The station bus can be redundant within PACiS. The switchover from a network to the other one is handled automatically by the system and is transparent for all PACiS equipment. The maximum switching time is 4 ms. It can be used DIN rail mounted switches or internal switches.

2.10.2.3 PACiS GTW redundancy

The transmission link of a gateway can be redundant to allow RCP to continue to control the substation in case of port single failure.

2.10.2.4 MiCOM C264 redundancy

At substation level and/or at bay level an optional second computer can be used to avoid the loss of functions at these levels. The two computers have the same configuration and support the same functions.

2.10.3 Local/remote control operating modes

2.10.3.1 Substation Local/Remote mode

A substation can be in remote control mode or local control mode.

The Remote mode indicates that the substation is controlled from RCP, via a gateway. No control can be sent from SCP level (except if the concerned bay is in SBMC mode, see below).

The Local mode indicates that the substation is controlled from PACiS OI. The controls issued from RCP are not taken into account by the system, they are refused.

Some controls, defined during the configuration phase, can be independent of the substation control mode: it means they can be issued from SCP or RCP whatever was the current control mode. Controls from configurable automation (ISAGRAF) are accepted whatever was the mode.

2.10.3.2 Bay Local/Remote mode

Each bay can be independently in Remote or Local mode.

The Remote mode indicates that the bay is controlled from the upper level (RCP or SCP depending on the current substation control mode). No control can be sent from BCP level.

The Local mode indicates that the bay is controlled from BCP. The controls issued from upper level are not taken into account by the bay.

Some controls, defined during the configuration phase, can be independent of the bay control mode: it means they can be issued from any control points whatever was the current control mode. Controls from configurable automation (ISAGRAF) are accepted in remote mode.

2.10.3.3 SBMC mode

You can set each bay in Site Based Maintenance Control (SBMC) mode.

A bay in SBMC mode does not take into account the commands issued from RCP, even if the substation is in remote control mode. All the information issued from the bay are sent to the SCP. Nevertheless for the RCP, PACiS system provides “automatic suppression” facility: by configuration some information of the bay are not sent to the RCP when the bay is in SBMC mode but a pre-configured value.

2.10.3.4 Local/Remote management on IEC/IEC Gateway

A configuration attribute allows you to define that the IEC61850 / IEC61850 gateway must use the Substation Local/Remote information. The Substation Local/Remote xPS comes from the lower IEC61850 network.

2.11 Engineering tools

The engineering tools, associated to PACiS, are used for configuration at system/equipment level.

Tools are used at different steps of the life cycle of a PACiS system and by different departments.

The PACiS system configuration is the core of the engineering toolset, the aim of this activity is to create and dispatch all the static data, objects, programmable functions and parameters into the MiCOM equipment.

2.11.1 System Configuration Editor (PACiS SCE)

There are two kinds of configuration activities:

- Modelling: this activity consists in the creation/modification of object classes and corresponds to a development phase of the PACiS system
- Manufacturing: this activity consists in the instantiation of objects to generate a PACiS system database according to a customer substation

The pre-configuration is constituted by the set of object models.

The configuration is constituted by the real objects of a PACiS system database.

2.11.1.1 Missions

The different missions of the system configuration are:

- create/update the objects for system devices according to customer and substation requirements
- check coherency and consistency between the objects before deployment into the system
- database versions management with the « delta » capability
- automatic documentation generation

2.11.1.2 Objects Modelling

The modelling define several families of objects which are handled by the system configuration:

- electrotechnical architecture objects which defines the substation topology (for example bays, switchgears, transformers, measurands)
- system architecture objects which defines the SCS architecture (for example equipment of the system)
- functions description objects which define the functions accomplished by the SCS (for example overcurrent protection function)
- real time exchanged data which define the communications between equipment and functions

2.11.2 Stand-alone Configuration Tool (SCT)

The Stand-alone Configuration Tool is based on the same principles than the SCE but is limited to the configuration of one computer. Nevertheless, some functions cannot be configured using this tool (refer to the SCT documentation)

2.11.3 C264 Maintenance Tool (CMT)

To simplify and secure the basic maintenance interventions on MiCOM C264s, the CMT is a PC-based graphical tool. It gives access to standard commands avoiding the use of shell.

The CMT communicates with MiCOM C264 on Ethernet in direct addressing mode. With CMT, the debug serial link is no more needed.

Two different configurations are available:

- maintenance (visualisation and modification for example Local access for computer maintenance)
- supervision (visualisation only: for example distance access)

2.11.4 Embedded Web maintenance server

For maintenance purposes a web server is embedded in MiCOM C264 equipped with a CPU270 (CPU3).

When connected (via a web browser) to this web server, you can get access to this data:

- Computer identification (name, Ethernet serial number, IP address 1 and 2)
- Software version, Software date, Database compatibilty
- Computer operating mode (OPERATIONAL / MAINTENANCE / TEST)
- Computer redundancy mode (ACTIVE / STANDBY / NOT REDUNDANT)
- Computer date and time
- Number of working hours for the MiCOM C264
- Database information (name, version and status (MAINTENANCE / CURRENT) for the two databases
- Status of each configured board (MISSING / PRESENT, CONFIGURED / NOT CONFIGURED, FAULTY / OK)
- Address of each board
- Status (ON / OFF) of the inputs of the configured BIU, DIU and CCU boards
- Status (OPEN / CLOSE) of the outputs of the configured BIU, DOU and CCU boards
- Number of operating hours
- C264 synchronisation status and IRIG-B status
- List of all IED configured with IED address and the legacy bus status (CONNECTED / DISCONNECTED)
- Status of the binary inputs
- Value and status of the measurements
- Status of the counters
- Status of the TPI.

2.12 PACiS Watch

2.12.1 Role

The function of PACiS Watch client is to launch and to watch the OI Client.

The function of PACiS Watch server is to launch and to watch the following tools:

- the “system tools” that are the main components of PACiS OI server: agency, OI Server, SMT_kernel and few other processes to be defined by the user and considered as essential;
- the “secondary tools”: additional processes with less importance than the previous ones, that the user wants to be started also at each time his application starts or at each PC boot.

In event of crash of a system tool, PACiS Watch restarts it automatically. But the event of more than a predefined number of crashes (by default 3) inside a predefined duration (by default 1 hour) the system tools crashes are considered too repetitive and Pacis Watch reboots the PC as default behaviour. As other possibility, it can stop itself after stopping all the watched tools, if the user prefers this option.

In event of crashes of the secondary tools, PACiS Watch restarts them systematically, independently of the number of crashes. Their crashes can’t lead to the PC reboot.

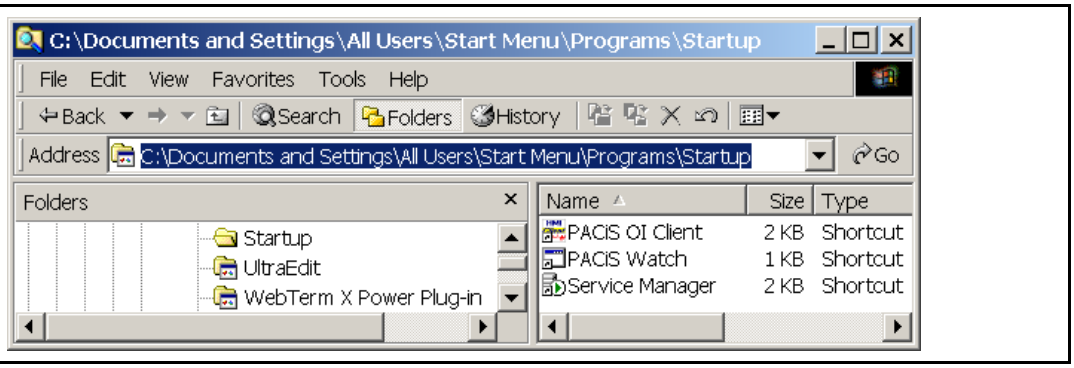
2.12.2 Use

2.12.2.1 Start

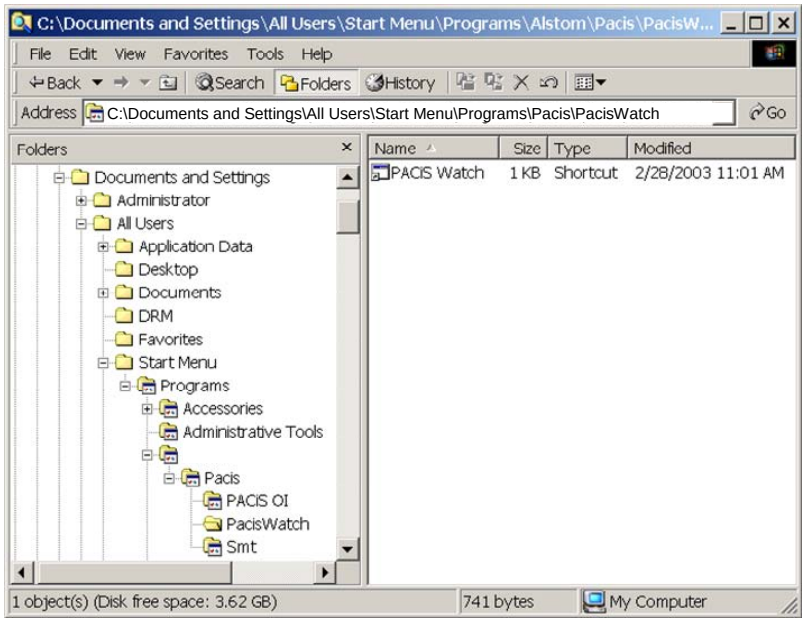
In this mode PacisWatch takes in account the PacisWatch.ini file located in C:\Program Files\PACIS\PacisWatch directory. It is possible to load and switch the BD with SMT.

There are two ways to launch PACiS Watch:

- at each PC boot via a PACiS Watch shortcut present in C:\Documents and Settings\All Users\Start Menu\Programs\Startup folder as shown below. So the final user does not have to launch PW himself/herself .



- by selecting the PACiS Watch item from the Start/Program menu; in this case the shortcut of the C:\Documents and Settings\All Users\Start Menu\... folder is activated, as shown below:



At its launch PACiS Watch triggers the start of the Pacis OI Server and potentially SMT_kernel and the potential other processes stated in the PacisWatch.ini file.

The state of processes and the crashes are logged in the PacisWatch.txt file, which is created in the directory, where PACIS Watch is installed.

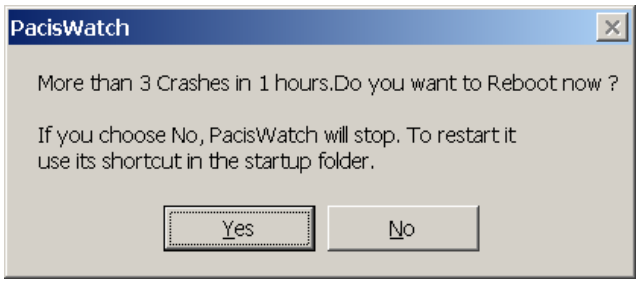
If this file size is more than 250 Kbytes at the beginning of a session, PACIS Watch copies this file as PacisWatch_Old.txt and create a new PacisWatch.txt file.

2.12.2.2 Number of crashes over the limit

If more crashes than the maximum number have occurred, there are several cases:

1. If the last one occurs inside the predefined time interval (H_hours), what happens depends on the value of the ConfirmBeforeReboot parameter:

- 0: there is no confirmation message box.
  - PACiS Watch stops the remaining watched processes and the PC shutdowns directly after a short apparition of a system information window indicating 30 seconds remain to possibly save files before the shutdown.
  - Then the PC reboots automatically. In this case the PACIS Watch shortcut is activated like the other shortcuts present in the start-up folder. In the next session of PACIS Watch the crashes count is re-initialised.
- 1: the following Message box proposes to the user to shutdown and reboot the station:


PacisWatch
More than 3 Crashes in 1 hours.Do you want to Reboot now ?
If you choose No, PacisWatch will stop. To restart it use its shortcut in the startup folder.
Yes
No

Yes: PACIS Watch stops the processes of the lists of the .ini file that are still running and then shutdowns after 30-second of timeout. Then the PC reboots automatically.

No for instance (by instance in integration phase): PACIS Watch stops all the watched processes and stops itself. Beware that, in this case, only a manual action can restart the application.

2. If the crash over the limit (N_crashes_inH) occurs later than the time interval (H_hours) started when the first crash occurred, no shutdown is triggered. Instead a new watch interval is started with this last crash considered as the first one (CRASH 1) of the period.

2.12.2.3 Quitting by a user

Different behaviours are possible when the user has manually stopped **OdcLoading** or **SMT_kernel** (using the Exit command available by right-click on the icon of either tool, in the system tray).

It is possible to configure PACiS Watch so that it restarts automatically this stopped tool, after a defined timeout, if the user has not yet restarted it. This depends on the value of the RestartAfterUserExit flag of the .ini file (see Settings in OI ENIN). The timeout duration after quitting also be set in the same way. By default there is no automatic restart of the two system tools.

2.13 Cybersecurity

2.13.1 General

There are 4 user profiles. The application will have up to 4 profiles protected by password so 4 roles are predefined. The login/password defines the menu that you can use. The password length could be extended to 8 digits.

Disable the unused application and physical ports.

You must disable all of the unused physical ports. You must disable all of the unused Ethernet ports.

Profile lockout: log off after x minutes of inactivity.

Store security logs: make a record of the date time and log duration. Circular buffer (size depends of the device).

Antivirus.

When you start an application, a disclaimer is displayed. Make sure that the user always knows where he operates. You can show a user banner if necessary.

3. PACiS ARCHITECTURES

The PACiS System architecture is always based on a Station Bus to which are connected PACiS & MiCOM equipments used for the customer solution. These equipments are:

- the Operator Workstation - PACiS OI
- the MiCOM C264
- the Telecontrol gateway – PACiS GTW
- the IEDs (protective devices, disturbance and quality recorder, **when available on Station Bus**)
- the Ethernet switches _MiCOM Hxxx
- the MiCOM Px3x & Px4x protection relays
- the MiCOM Mx7x measurement units

The Station Bus is based on the IEC61850 protocol, over an Ethernet / TCP-IP network. Additional busses (called legacy busses) are also available in the PACiS System architectures.

The structure of MiCOM equipment is:

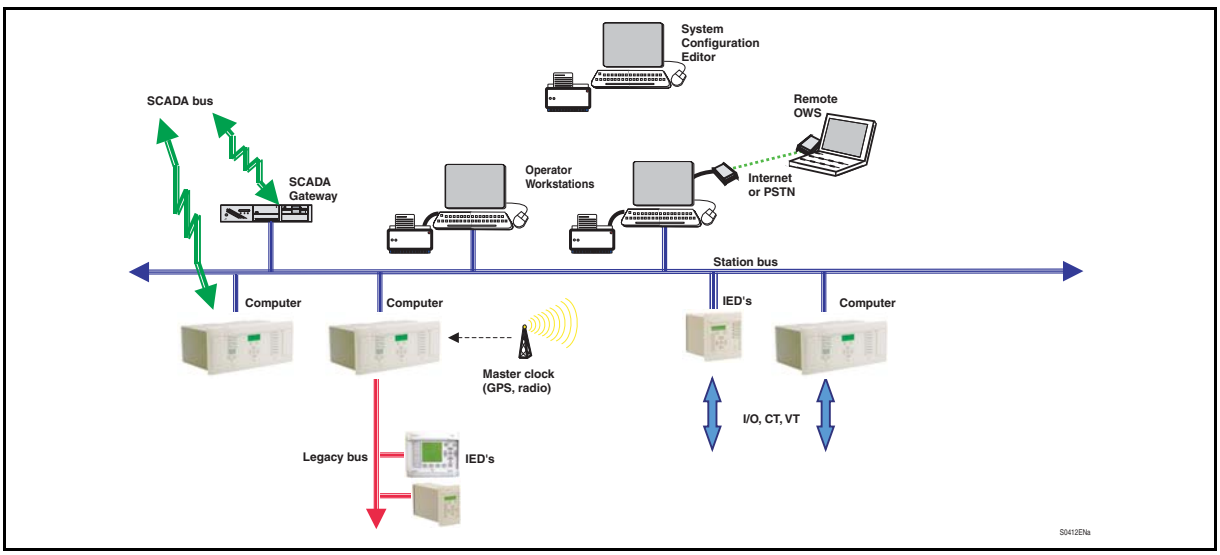
- rack-based for MiCOM C264
- rack-based for all MiCOM P and M available over Ethernet
- PC-based for PACiS GTW Telecontrol Interface and PACiS OI Operator Workstation
- MiCOM Hxxx Ethernet switch, this equipment is used for Ethernet redundancy

Any combination of equipment around the Station Bus is allowed to match with the required application.

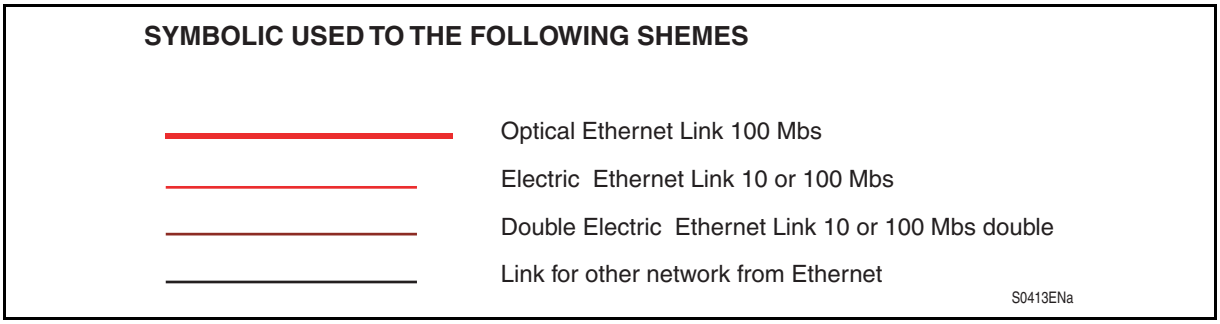
The typical **PACiS** architecture consists in a series of devices connected over the ETHERNET communication network, in order to:

- maximise the functional integration through fast exchanges between devices (10/100 Mbps)
- allow a flexible distribution inside or between substations
- integrate third party devices within the Digital Control System of the substation

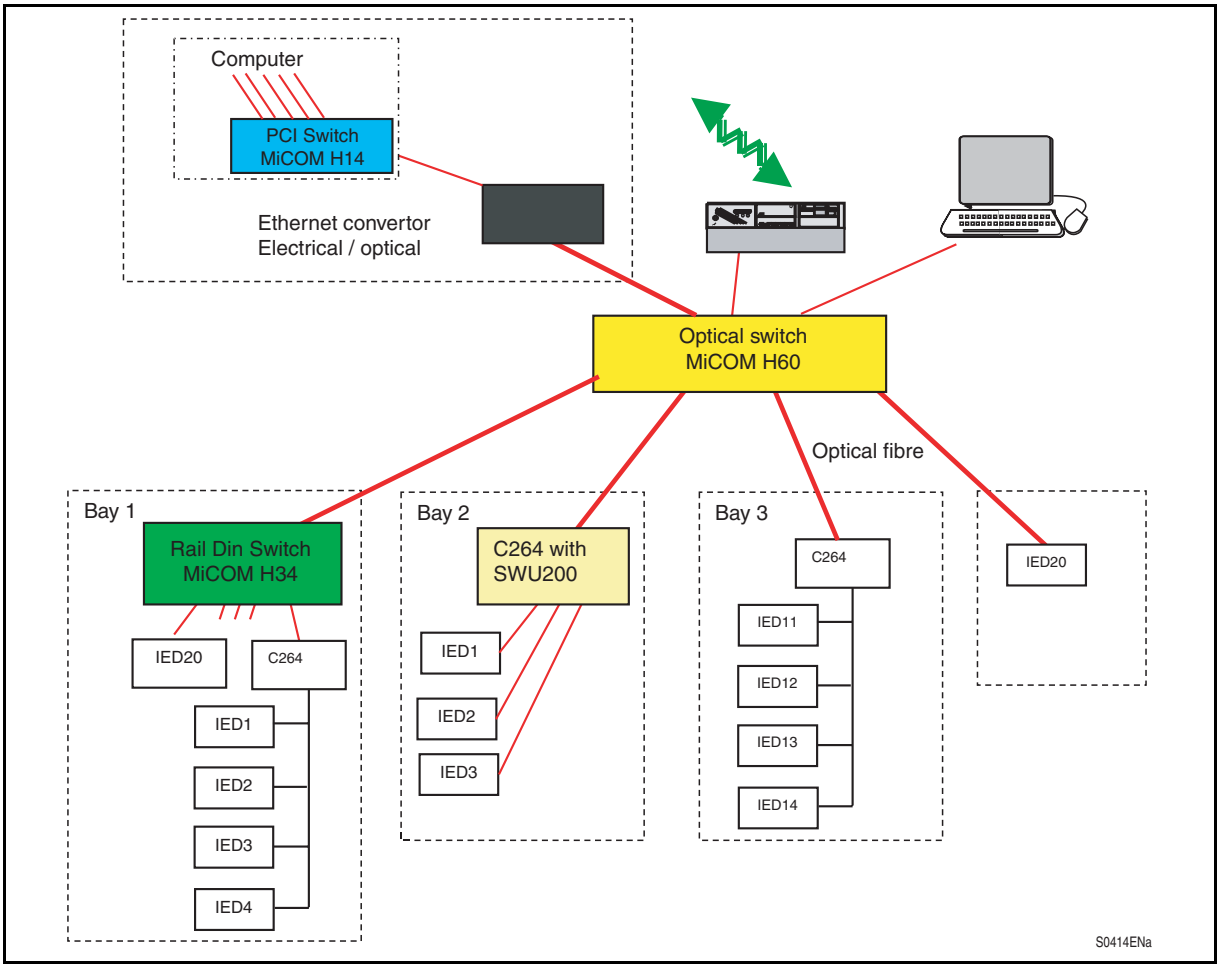
PACiS offers connection with legacy communication networks (RS232, RS485, optical) in order to fully re-used past investments with the new generation.



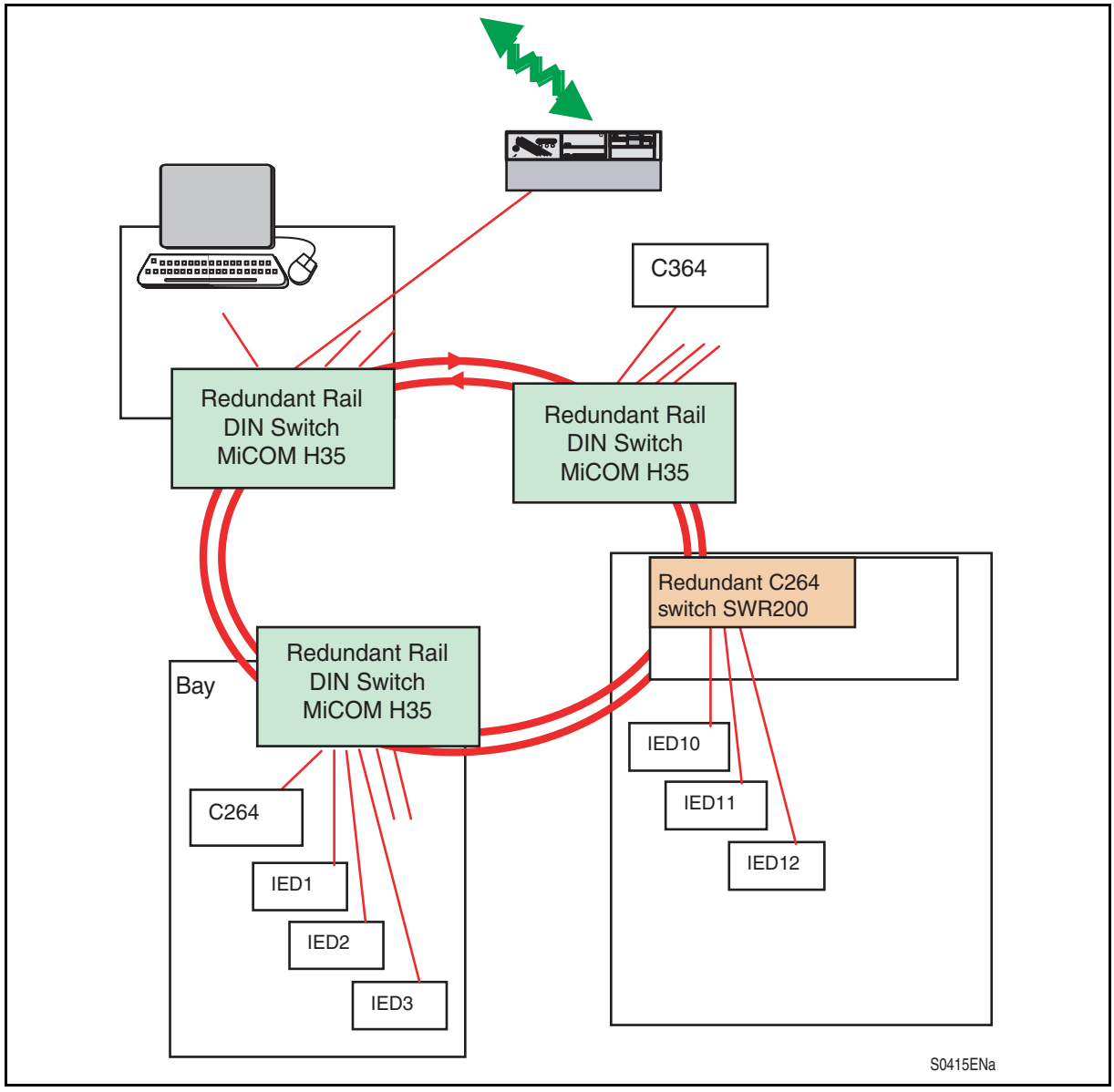
4. PACiS ETHERNET NETWORK ARCHITECTURES


SYMBOLIC USED TO THE FOLLOWING SHEMES
Optical Ethernet Link 100 Mbs
Electric Ethernet Link 10 or 100 Mbs
Double Electric Ethernet Link 10 or 100 Mbs double
Link for other network from Ethernet
S0413ENa

4.1 Simple star network

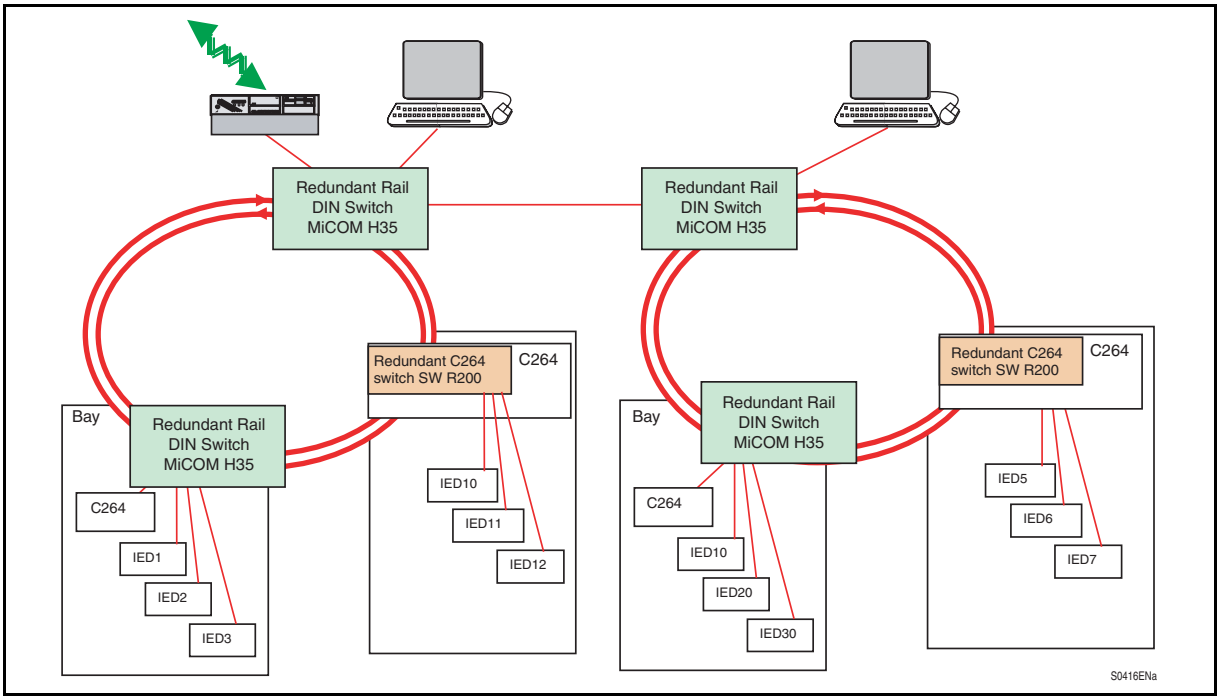


4.2 Redundant optical ring network

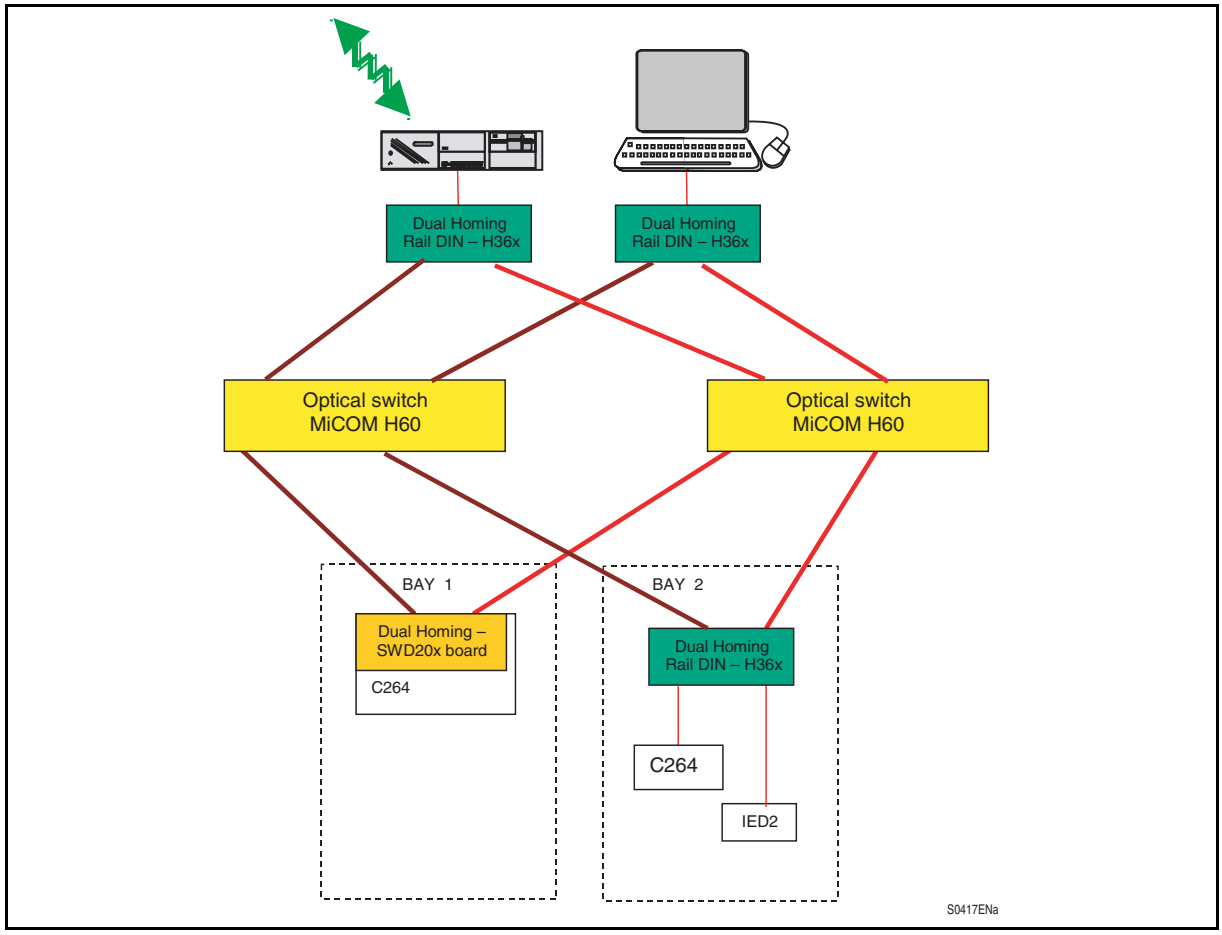


Use of double ring

In order to optimise the data flow on the network this one is split in more than one ring. The link between the rings is made by two switches.



4.3 Dual Homing network



The Dual Homing architecture can also be used with a ring architecture with additional electrical / optical Ethernet converters.

4.4 Virtual LAN

PACiS V4.8 offers the capability to send information on Physical VLAN according to the recommendations in Annex C of IEC61850-8-1.

The default virtual LAN IDs and priorities are described below:

Service	Default VLAN VID	Default VLAN Priority
GOOSE	0	4
GSE (Events)	0	1
Sampled Values	0	4

Please refer on SCE Chapter AP for setting.

5. MULTI-LINGUAL SUPPORT

5.1 Italian Language

These sub-systems support the Italian language:

- SCE: only the menus and the capability to configure the Italian language. The data model is not translated
- CMT
- SMT
- PACiS S1
- OI: the default reports do not support the Italian language.

These components do not support the Italian language:

- The C264 local HMI
- The user documentation
- The program installation set-up files and displays.

5.2 Greek Language

These sub-systems support the Greek language:

- The OI is translated in Greek, including the pre-defined reports
- The SCE allows you to select the Greek language and to create Greek datapoint labels. The system data model of the SCE is not translated into Greek

Note: All of the other PACiS sub-systems are not translated into Greek.

BLANK PAGE

LEXICAL

CONTENT

1.	**SCOPE OF THE DOCUMENT**	**3**
2.	**LEXICAL**	**4**

BLANK PAGE

1. SCOPE OF THE DOCUMENT

This document is the last chapter of each PACiS documentation. It is the lexical.

2. LEXICAL

AC	Alternating Current
AccI	Accumulator Input
ACSI	Abstract Communication Service Interface Mapping from the standard IEC61850 abstract specification of communication service to a concrete communication infrastructure based on CORBA specific.
A/D	Analog/Digital
ADC	Analogue to Digital Converter
AE qualifier	Application Entity qualifier (Used internally by IEC61850 to identify a server Application)
AI	Analogue Input (Measurement Value including state attribute) Commonly Voltage or current DC signals delivered by transducers, and representing an external value (refer to CT/VT for AC).
AIS	Air Insulated Substation
AIU	Analogue Input Unit (Computer C264 Board name for DC Analogue Input)
Alarm	An alarm is any event tagged as an alarm during configuration phase
AO	Analogue Output Value corresponding to a desired output current applied to a DAC.
AOU	Analogue Output Unit (computer C264 board name for Analogue Output)
API	Application Programming Interfaces
AR	Auto-Reclose
ARS	Auto-Recloser
ASCII	American Standard Code for Information Interchange
ASDU	Application Specific Data Unit Name given in OSI protocol for applicative data (T103, T101..)
ASE	Applied System Engineering
ATCC	Automatic Tap Change Control Automation in charge of secondary voltage regulation, more specific than AVR
AVR	Automatic Voltage Regulator Automatism used to regulate secondary voltage by automatic tap changer control (see ATCC). Set of features can be added, see chapter C264 FT
Bay	Set of LV, MV or HV plants (switchgears and transformers) and devices (Protective, Measurement…) usually around a Circuit Breaker and controlled by a bay computer.
BCD	Binary Coded Decimal One C264 supported coding on a set of Digital Inputs, that determine a Digital Measurement, then Measurement value (with specific invalid code when coding is not valid). Each decimal digit is coded by 4 binary digits.
BCP	Bay Control Point Name given to the device or part used to control a bay. It can be Mosaic Panel, C264 LCD,… Usually associate with Remote/Local control.
BCU	Bay Control Unit Name given to the C264 in charge of a bay. Usually in contrast with Standalone

BI	Binary Input (or Information) Name given into Computer C264 of information already filtered, before it becomes an SPS, DPS… with time tag and quality attributes
BIU	Basic Interface Unit C264 Board for auxiliary power supply, watchdog relay, redundancy I/O
BNC	A connector for coaxial cable.
B-Watch	Monitoring and control device for GIS substation.
CAD	Computer Aided Design Computer application dedicated to design like wiring, protective setting…
CAS	CASe Computer C264 rack
CB	Circuit Breaker Specific dipole switch with capability to make line current and break fault current. Some have isolation capability (nominal-earth at each side)
CBC	Compact Bay Controller Small capacity bay computer for Medium Voltage applications typically C264C
CC	Complemented Contact
CCU	Circuit breaker Control Unit Computer C264 Board dedicated to switch control with 8DI, 4 DO
CDM	Conceptual Data Modelling Is the modelling of system/devices data using a hierarchy of structured data (called object of class) with their attributes, method or properties and the relations between themselves. It maps common data to devices or components of devices, with guaranty of interoperability.
Class	Define in IEC61850 as: description of a set of objects that share the same attributes, services, relationships, and semantics
Client	Define in IEC61850 as: entity that requests a service from a server and that receives unsolicited messages from a server
CM	CoMissioning
CMT	Computer Maintenance Tool
CO	Command, logic information Output (Functional Component) / Contact Open
COMTRADE	Common Format For Transient Data Exchange (international standard IEC 60255-24)
CPU	Central Processing Unit Computer C264 main Board based on PowerPC
CRC	Cyclic Redundancy Check Coding result send with packet of transmitted data to guarantee their integrity. Usually result of a division of transmitted data by polynomial.
CSV	Character Separate Values ASCII values separated by predefined character or string like in Excel or ASCII Comtrade.
CT	Current Transformer Basically the electric device connected to process and extracting a current measurement. By extension part of a device (C264) that receives AC values and convert it to numerical measurement value.
CT/VT (Conventional)	Current and Voltage transformers By extension, it is the C264 TMU board.

CT/VT (Non-Conventional or intelligent)	Current and Voltage transformers New generation of captor based for example on light diffraction under electric field, without transformer, that gives directly numerical measurement of voltage and current like communicating IED.
CSV	Character Separate Values Asci values separated by predefined character or string like in Excel or ASCII Comtrade.
DAC	Data Acquisition component of the GPT
DAC	Digital to Analogue Converter Used to generate analogue signals (usually DC) from a digital value.
DB	DataBase Tool or set of data that define all configuration of a system or specific device like computer. Opposed to setting or parameter DB has a structure that can not be modified on line. DB are always versioned.
DB-9	A 9-pin family of plugs and sockets widely used in communications and computer devices.
DBI	Don't Believe It Term used for undefined state of a double point when input are not complementary. DBI00 is state motion or jammed. DBI11 is undefined.
DBID	Databases Identity Brick
DC	Direct Current
DC, DPC	Double (Point) Control Two digit and/or relays outputs used for device control with complementary meaning (OPEN, CLOSE).
DCF77	External master clock and protocol transmission LF transmitter located at Mainflingen, Germany, about 25 km south-east of Frankfurt/Main, broadcasting legal time on a 77.5 kHz standard frequency.
DCO	Double Control Output
DCP	Device Control Point Located at device level (electric device or IED). It should have its own Remote/Local switch.
DCS	Digital Control System Generic name of system based on numeric communication and devices, to be opposed to traditional electrically wired control.
DCT	Double CounTer Counter based on 2 DI with complementary states (counting switchgear manoeuvre for example)
DE	Direct Execute
DELTA	Phase to phase delta values
Device	Term used for one of the following unit: Protective relays, metering units, IED, switchgear (switching device such as CB, disconnector or earthing switch), disturbance or quality recorders.
DHMI	C264 Display HMI
DI	Digital Input Binary information related to the presence or to the absence of an external signal, delivered by a voltage source.
DIN	Deutsche Institut für Normung The German standardisation body.
DIU	DC Input Unit Computer C264 Board name for Digital Input

DLL	Dynamic Link Library. Available on Windows XP. A feature that allows executable code modules to be loaded on demand and linked at run time. This enables the library-code fields to be updated automatically, transparent to applications, and then unloaded when they are no longer needed.
DM	Digital Measurement Is a measurement value which acquisition is done by DI and a specific coding BCD, Gray, 1 among N…
DNP3.0	Distributed Network Protocol DNP3 is a set of communication protocols used between components in process automation systems.
DO	Digital Output Used to apply a voltage to an external device via a relay, in order to execute single or dual, transient or permanent commands.
DOF	Degree Of Freedom Used for a template attribute, that can be modified or not when used. An attri-bute has a degree of freedom if a user can modify its values on its instances
DOU	Digital Output Unit Computer C264 Board name for Digital Output
DP	Double Point Information/control derived from 2 digital inputs/output; usually used for position indication of switching devices (OPEN, CLOSE).
DPC	Double Point Control
DPS	Double Point Status Position indication of switching devices (OPEN, CLOSE).
ECDD	Coherent Extract of Distributed Data
ECU	Extended Communication Unit. External module connected to the CPU board. This module converts non-insulated RS232 into optical signal or insulated RS485/RS422.
EH90	Transmission protocol dedicated to time synchronisation and standardised by EDF. Specification document: D.652/90-26c, March 1991.
EMC	Electro-Magnetic Compatibility
EPATR	Ensemble de Protection Ampèremétrique de Terre Résistante (French Legacy very resistive earth current module)
Event	An event is a time tagged change of state/value acquired or transmitted by a digital control system.
FAT	Factory Acceptance Test Validation procedures execution with the customer at factory.(i.e. SAT)
FBD	Functional Block Diagram One of the IEC61131-3 programming languages (language used to define configurable automation).
FIFO	First In First Out
FO	Fibre Optic
FP	Front Panel
FTP	Foil Twisted Pair
FLS	Fast Load Shedding
FSS	Force Suppress Substitute

Gateway	Level 6 session of OSI, the gateway is any device transferring data between different networks and/or protocol. The RTU function of the C264 gives a gateway behaviour to SCADA or RCP level. PACIS Gateway is separate PC base device dedicated to this function.
GHU	Graphic Human interface Unit Computer C264 Front Panel digital part (LCD, buttons, Front RS)
GIS	Gas Insulated Substation
GLOBE	GLOBE Brick
GMT	Greenwich Mean Time Absolute time reference
GPS	Global Positioning System Based on triangulation from satellite signal, that transmit also absolute GMT time used to synchronise a master clock
GOOSE	Generic Object Oriented Substation Event
GPT	Generic Protocol Translator software, supplied by ASE
Group	Logical combination of BI (i.e. SP, DP, SI or other groups).
GSSE	Generic Substation Status Event
Hand Dressing	Facility for an operator to set manually the position of a device (acquired by other means) from the HMI at SCP level; e.g. from OPEN to CLOSE (without any impact on the “physical” position of the electrical switching device).
HMGA	Horizontal Measurement Graphical Area
HMI	Human Machine Interface Can be PACIS OI (Operator Interface) or C264 LCD (Local Control Display) or Leds, mosaic...
HSR	High Speed auto-Recloser, first cycles of AR
HTML	Hyper Text Mark-up Language Used as standard for formatting web display
HV	High Voltage (for example 30kV to 150kV)
I/O	Input/Output
ICD	IED Capability Description
IEC	International Electro-technical Commission
IED	Intelligent Electronic Device General expression for a whole range of microprocessor based products for data collection and information processing
IP	Internet Protocol
IRIG-B	Inter-Range Instrumentation Group standard format B. This is an international standard for time synchronisation based on analogue signal.
JAMMED	Invalid state of a Double Point: Occurs when the 2 associated digital inputs are still in state 0 after an user- selectable delay, i.e. when the transient state “ motion ” is considered as ended
Kbus (Kbus Courier)	Term used for the protocol Courier on K-Bus network (kind of RS422).
LAN	Local Area Network

L-BUS	Legacy Bus Generic name of Legacy or field networks and protocols used to communicate between C264 (Legacy Gateway function) and IED on field bus. Networks are based on (RS232,) 422, 485. Protocols are IEC 60850-5-103 (T103 or VDEW), Modbus Schneider Electric or MODICON
LCD	Liquid Crystal Display or Local Control Display (on C264)
LD	Ladder Diagram, one of the IEC1131-3 programming languages (language used to define configurable automation).
LED	Light Emitting Diode
LF	Low Frequency
LOC	Local Operator Console Dedicated to maintenance operation
L/R	Local / Remote
Local / Remote Control Mode	When set to local for a given control point it means that the commands can be issued from this point, else in remote control are issue for upper devices.
LSB	Least Significant Bit
LSP	Load Shedding Preselection
LV	Low Voltage
MAFS	Marketing And Functional Specification
MC	Modular Computer
MCB	Mini Circuit Breaker. Its position is associated to tap changer.
MDIO	Management Data Input/Output A standard driven, dedicated-bus approach that is specified in IEEE802.3
Measurements	Values issued from digital inputs or analogue inputs (with value, state, time tag)
Metering (non-tariff)	Values computed depending on the values of digital or analogue inputs during variable periods of time (time integration).
Metering (tariff)	Values computed depending on the values of digital or analogue inputs during variable periods and dedicated to the energy tariff. These values are provided by dedicated “tariff computer ” which are external to the MiCOM Systems.
MIDOS	Schneider Electric Connector: Used for CT/VT acquisition
MMC	Medium Modular Computer
MMS	Manufacturing Message Specification (ISO 9506)
ModBus	Communication protocol used on secondary networks with IED or with SCADA RCP. 2 versions exist with standard MODICON or Schneider Electric one.
Module	Word reserved in PACIS SCE for all electric HV devices. It groups all switch-gears, transformer, motors, generators, capacitors, …
MOTION	Transient state of a Double Point Occurs when the two associated digital inputs are momentarily in state 0 (e.g. position indication when an electrical device is switching). The concept of “momentarily” depends on a user-selectable delay.
MPC	Protection Module for Computer
MV	Medium Voltage
MVAR	Mega Volt Ampere Reactive
NBB	Numerical Busbar Protection

NC	Normally Closed (for a relay)
NO	Normally Open (for a relay)
OBS	One Box Solution Computer that provides protection and control functions with local HMI. The prime application of this device is intended for use in substations up to distribution voltage levels, although it may also be used as backup protection in transmission substations. Likewise, the OBS may be applied to the MV part of a HV substation that is being controlled by the same substation control system.
OI	Operator Interface
OLE	Object Linking and Embedding OLE is a Microsoft specification and defines standards for interfacing objects.
OLTC	On Line Tap Changing
OMM	Operating Mode Management
OPC	OLE for process control OPC is a registered trademark of Microsoft, and is designed to be a method to allow business management access to plant floor data in a consistent manner.
Operation hours	Sum of time periods, a primary device is running under carrying energy, e.g. circuit breaker is in Close state and the current is unequal 0 A.
OSI	Open System Interconnection Split and define communication in 7 layers : physical, link, network, transport, session, presentation, application
OWS	Operator WorkStation (PACiS OI)
PACiS	Protection, Automation and Control Integrated Solutions
PLC	Programmable Logic Control /Chart. Includes PSL and ISaGRAF Within the PLC-programs are defined the configurable control sequences or automations taken into account by the MiCOM Systems.
POW	Point On Wave Point on wave switching is the process to control the three poles of an HV-circuit breaker in a way, to minimise the effects of switching.
PSL	Programmable Scheme Logic
PSTN	Public Switched Telephone Network
RCC	Remote Control Centre Is a computer or system that is not part of PACiS MiCOM system. RCC communicates with and supervises PACiS MiCOM system using a protocol.
RCP	Remote Control Point Name given to the device or part used to control remotely several bay or sub-station. Usually associated with Remote/Local sub-station control. It is a SCADA interface managed by the MiCOM system through Telecontrol BUS. Several RCPs can be managed with different protocols.
Remote Control Mode	When set for a control point it means that the commands are issued from an upper level and are not allowed from this point.
Remote HMI	Remote HMI is a client of the substation HMI server. The client may provide all or part of functions handled by the substation HMI.
RI	Read Inhibit This output indicates the availability of an analogue output (e.g. during DAC converting time)
RJ-45	Registered Jack-45 A 8-pin female connector for 10/100 Base-T Ethernet network

RMS	Root Mean Square
RRC	Rapid ReClosure
RSE	Régime Spécial d'Exploitation French grid function when works are being done on a HV feeder
RSVC	Relocatable Static Var Compensator
RS-232	Recommended Standard 232 A standard for serial transmission between computers and peripheral devices.
RS-422	A standard for serial interfaces that extends distances and speeds beyond RS-232. Is intended for use in multipoint lines.
RS-485	A standard for serial multipoint communication lines. RS-485 allows more nodes per line than RS-422
RSVC	Relocatabled Static Var Compensator
RTC	Real Time Clock
RTU	Remote Terminal Unit Stand alone computer that acquires data and transmit them to RCP or SCADA. Typically it is the C964. RTU link is the TBUS.
SAT	Site Acceptance Test Validation procedures executed with the customer on the site.
SBMC	Site Based Maintenance Control mode A bay in SBMC mode does not take into account the commands issued from RCP; moreover, some of its digital points & measurements (defined during the configuration phase) are not sent anymore to the RCP (they are "automatically" suppressed).
SBO	Select Before Operate A control made in two steps, selection and execution. Selection phase give a feedback. It can be used to prepare, reserve during time, configure circuit before execution. Controls are done into a protocol, or physical (DO select with DI Select then DO execute).
S-BUS	Station Bus, federal network between PACIS devices.
SCADA	Supervisory Control And Data Acquisition Equivalent to RCC
SCD	Description file extension (SCE)
SCE	System Configuration Editor
SCL	substation automation System Configuration Language (IEC 61850-6)
SCP	Substation Control Point Name given to the device or part used to control locally several bays or sub-station. Usually associated with Remote/Local sub-station control. It is commonly PACIS Operator Interface.
SCS	Substation Control System
SCSM	Specific Communication Service Mapping
SCT	Single Counter
SER	Sequence of Event Recorder Combines SOE with accurate Time synchronization and Maintenance facilities over Ethernet communication
Server	Define in IEC61850 as: entity that provides services to clients or issues unsolicited messages

Setpoints (analogue)	Analogue setpoints are analogue outputs delivered as current loops. Analogue setpoints are used to send instruction values to the process or auxiliary device
Setpoints (digital)	Digital values sent on multiple parallel wired outputs Each wired output represent a bit of the value. Digital setpoints are used to send instruction values to the electrical process or to auxiliary devices.
SFC	Sequential Function Chart One of the IEC1131-3 programming languages (language used to define configurable automation).
SI	System Indication Binary information that do not come from external interface. It is related to an internal state of the computer (time status, hardware faults…). It is the result of all inner function (AR, …), PSL, or ISaGRAF automation.
SICU 4	Switchgear Intelligent Control Unit Control unit of an intelligent circuit breaker (fourth generation)
SIG	Status Input Group
SINAD	Signal-plus-Noise-plus-Distorsion to Noise-plus-Distorsion ratio, in dB
SIT	Status Input Double Bit
SNTP	Simple Network Time Protocol
SOE	Sequence Of Events Other term for the event list.
SP SPS SPC	Single Point Single Point Status Single Point Control
ST	Structured Text An IEC1131-3 programming language to define configurable automation
STP	Shielded Twisted Pair
Substation computer	Bay computer used at substation level
Suppression (Automatic)	A binary information belonging to a bay in SBMC mode will be automatically suppressed for the remote control. However changes of state will be signalled locally, at SCP
Suppression (Manual)	A binary information can be suppressed by an order issued from an operator. No subsequent change of state on a “suppressed information ” can trigger any action such as display, alarm and transmission
SWR	Switch Redundant Computer C264 board Ethernet switch with redundant Ethernet
SWU	Switch Unit (Computer C264 board Ethernet switch)
T101	Term used for IEC60870-5-101 protocol
T103	Term used for IEC60870-5-103 protocol
T104	Term used for IEC60870-5-104 protocol
TBC / TBD	To Be Completed / Defined
T-BUS	Telecontrol Bus, generic name of networks and protocols used to communicate between PACIS Gateway or C264 Telecontrol Interface function and the RCP. Networks are based on RS232, 485, or Ethernet (T104). Protocols are IEC 60850-5-101 (T101), Modbus MODICON
TC	True Contact
TCIP	Tap Changer in Progress

TCU	Transformer Current Unit Computer C264 CT/VT Board : Current acquisition
TDD	Total Demand Distorsion, similar to the THD but applied to currents and with a rated current (I_n) as reference
TG	Telecontrol Gateway
THD	Total Harmonic Distorsion, sum of all voltage harmonics
TI	Tele Interface
TM	Analogue Measurement
TMU	Transducerless Measurement Unit
Topological interlocking	Interlocking algorithm, based on evaluation of topological information of the switchgear arrangement in the HV network, the switchgear kind and position, & defined rules for controlling this kind of switch (e.g. continuity of power supply)
TPI	Tap Position Indication (for transformers). Frequently acquired via a Digital Measurement
TS	Logic position
TVU	Transformer Voltage Unit (computer C264 CT/VT Board : Voltage acquisition)
UCA	Utility Communications Architecture Communication standard (mainly US) used for PACIS SBUS communication
UPI	Unit Per Impulse Parameter of counter to convert number of pulse to Measurement value. Both data (integer and scaled float) are in common class UCA2 Accumulator.
UTC	Universal Time Co-ordinates (or Universal Time Code) Naming that replace GMT (but it is the same)
VdBS	Versioned data Base System, databag generated by SCE & ready to download
VDEW	Term used for IEC60870-5-103 protocol
VMGA	Vertical Measurement Graphical Area
Voltage level	Set of bays whose plants & devices are dealing with same voltage (e.g. 275kV)
VT	Voltage Transformer Basically the electric device connected to process and extracting a voltage measurement. By extension part of a device (C264) that receives this AC value and convert it to numerical measurement value. VT are wired in
WTS	Windows Terminal Server, Microsoft's remote desktop connection
WYE	Three phases + neutral AI values

BLANK PAGE

CYBER SECURITY

CONTENTS

1.	**SCOPE OF THE DOCUMENT**	**3**
2.	**GLOSSARY AND DEFINITIONS**	**4**
3.	**DOCUMENTATION REFERENCE**	**5**
4.	**RESPONSIBILITIES AND RECOMMENDATIONS**	**6**
4.1	**On demand PC based application**	**6**
4.2	**Permanent PC based application**	**6**
4.3	**Additional Recommendation Gateway**	**6**
4.4	**C264 computer**	**6**
4.5	**Additional Recommendation Switchs**	**6**
4.6	**Applications out of cyber security scope**	**6**
5.	**CYBERSECURITY POLICY**	**7**
5.1	**Applicability**	**7**
5.2	**Disclaimer**	**8**
5.3	**Banner**	**8**
5.4	**Password**	**8**
5.4.1	Password strength	8
5.4.2	Privileges	9
5.4.3	Profile lockout	9
5.4.4	Default password	10
5.5	**Log off after x minutes of inactivity**	**10**
5.6	**Device hardening and EWF**	**11**
5.7	**Security logs**	**11**
5.8	**Antivirus**	**12**
6.	**APPENDIX**	**13**
6.1	**Port reservation**	**13**

BLANK PAGE

1. SCOPE OF THE DOCUMENT

This document describes the measures taken and tools to decrease the risk of attacks and ensure Confidentiality, Integrity, Availability / Authentication and Non-Repudiation.

For more detail on implementation of the principles for the various components, refer to:

- CAT and the C264 cyber security
- SMT/EN IN chapter
- OI/EN IN chapter
- GTW/EN IN chapter

2. GLOSSARY AND DEFINITIONS

Authentification	Information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.
Availability	For any information system to serve its purpose, the information must be available when it is needed.
Banner	Configurable indication which allows the user to identify the device.
BCU	Bay Control Unit.
CAT	Computer Administration Tools.
Cyber security	Security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber securtity attacks.
Cyber security scope / perimeter	It is assumed that security perimeter is the cubicle.
Device	Can be gateway or C264.
DHMI	C264 Display HMI.
Disclaimer	Legal text of about 100 characters available in English only. This text is displayed at each start-up of the application and allows the application to run only if the text is acknowledged by a manual operation. The disclaimer is a message shown to the user, to transfer the usage responsibility to the user. (Misuse, unauthorized use…) It is a contract that user must accept before accessing to “temporary application”.
EWF	The Enhanced Write Filter (or EWF) is a component of Windows XP Embedded which filters writes to another medium instead of being physically written to the volume itself. Data integrity is composed of four essential qualities or core attributes: completeness, currency/timeliness, accuracy/correctness and validity/authorization.
ICD	IED Capability Description.
IED	Intelligent Electronic Device.
Integrity	In information security, integrity means that data cannot be modified undetectably.
Login/password	Way to identify a user. Login/password is associated to a unique account.
MS1	MiCOM C264 setting tools.
NERC	The North American Electric Reliability Corporation.
OI	Operator Interface.
Profile	List of functionalities.
SCE	System Configuration Editor.
SMT	System Management Tool.
User	A physical person.

3. DOCUMENTATION REFERENCE

Not Applicable.

4. RESPONSIBILITIES AND RECOMMENDATIONS

4.1 On demand PC based application

Definition: **On demand PC based applications** launched from a laptop or not exclusively PACIS applications are considered as Temporary PC based application in PACiS Systems, SMT Client, MiCOM S1 and CAT.

- Unused Ports: Operator has the responsibility to close the other ports not used by applications in order to secure access (refer on Appendix on section Port reservation).
- Antivirus: PACiS applications are authorized to run with the condition an antivirus is installed. Operator has the responsibility to realize the PC scanning and antivirus updating.

4.2 Permanent PC based application

Definition: Time-critical applications running permanently on a PC like: PACiS GTW (without HMI), PACIS SMT kernel are considered as **Permanent PC based application**.

- Unused Ports: Addressed through good installation practices of windows Operating system is recommended; refer on section Device hardening and EWF.
- Antivirus: Due to time-critical applications, antivirus installation is not recommended; The PACIS CYBER tool for software updating and PC scanning is recommended.

4.3 Additional Recommendation Gateway

- Operator has the responsibility to define firewall, entering flow and segregation of the traffic.
- Cyber security recommendations are involved by good practices of windows Operating System installation (best practices are indicated by **Schneider-Electric Platform Microsoft Windows XP hardening** recommendations).

4.4 C264 computer

- No recommendation because the C264 computer is running on a specific hardware and base on non Windows OS.

4.5 Additional Recommendation Switchs

- Switch Manager: recommendation to install it on **Windows machine secure**.
- Operator has the whole responsibility to define the cyber security policy.

4.6 Applications out of cyber security scope

Applications **PACiS OI and PACiS SCE are out of scope of cyber security**.

5. CYBERSECURITY POLICY

The minimum Cyber Security policy includes:

- Disclaimer and banner
- Password use with different profiles (or roles)
- Device hardening (unused ports) and EWF
- Security logs
- Antivirus

5.1 Applicability

The synthetic requirements for each application inside the cyber security scope are described on this table below. The presentation of requirements is described on next sections.

	Permanent PC-based application		**On demand PC-based application**	**Embedded application**
Requirement	**SMT kernel**	**GTW**	**CAT / MiCOM S1 / SMT Client**	**C264**
Disclaimer	-	-	A disclaimer is displayed at launch	-
Banner	-	-	Before any IED operation, invitation to read IED banner to increase awareness SMT client: –	Banner (shown on MiCOM S1 & CAT)
Profiles (password)	1	1	MiCOM S1: 1 SMT client: 3 CAT: 4	DHMI: 2
Profile lockout Log off	X	X	X	X
Unused ports	-	-	X	X
EWF	-	X	-	-
Security logs	X	X	X	X
Antivirus	Not recommended PACiS CYBER Tool recommended		Strongly recommended	-

X : Requirement exis
– : Requirement does not exist

5.2 Disclaimer

The disclaimer is a message shown at launch to transfer the usage responsibility to the user. To access to the application, the user must accept this contract, written in the software language.

Disclaimer
Access to this system is limited to specifically authorized users having received all trainings required by applicables laws, regulations, and by policies and procedures implemented by the legal entity hosting this system.
Unauthorized users may face criminal or civil liabilities and/or penalties. The use of this system may be recorded and monitored for system operations, security policy and intellectual property compliance related purposes and any information related to the use of this system may further be disclosed to third parties or law enforcement officials as necessary.
Disconnect now if you are not an authorized user or do not agree with the above terms.
I Agree
I Disagree

Press the button **I Agree** to move on. Pressing **I Disagree** causes the program to close.

5.3 Banner

The banner is an easy-to-read message that plainly identifies the device where the user is connected / working to prevent him/her from mistaking it for another one.

It is stored in C264 or the connected PC.

The banner is fixed whatever language is selected; it is configurable in SCE:

- It contains at least 32 characters, at most 6 lines and 10 characters by line,
- It can be the start and/or inactivity (screen saver) C264 panel to comply with the NERC standard, or neither.

5.4 Password

A password is required to place a command or set a parameter (whether from the front panel or via a PC-based application). For this purpose, at some point, the user chooses a profile that depends on the intended activity.

Access without a proper password is denied as soon as the security administrator has defined the passwords.

5.4.1 Password strength

It is recommended to comply with the NERC standards; for this purpose, the password must have 8 caracters and in addition contains at least one character from all the categories that follow:

- Upper case characters (A-Z)
- Lower case characters (a-z)
- Base 10 digits (0-9)
- Non-alphanumeric, that is:

!	"	#	$	%	&	'	(	)	*	+	,	-	.
/	:	;	<	=	>	?	@	[	\	]	^	_	`

5.4.2 Privileges

A profile (or role or account) is a set of privileges. Its name is referred to as login.

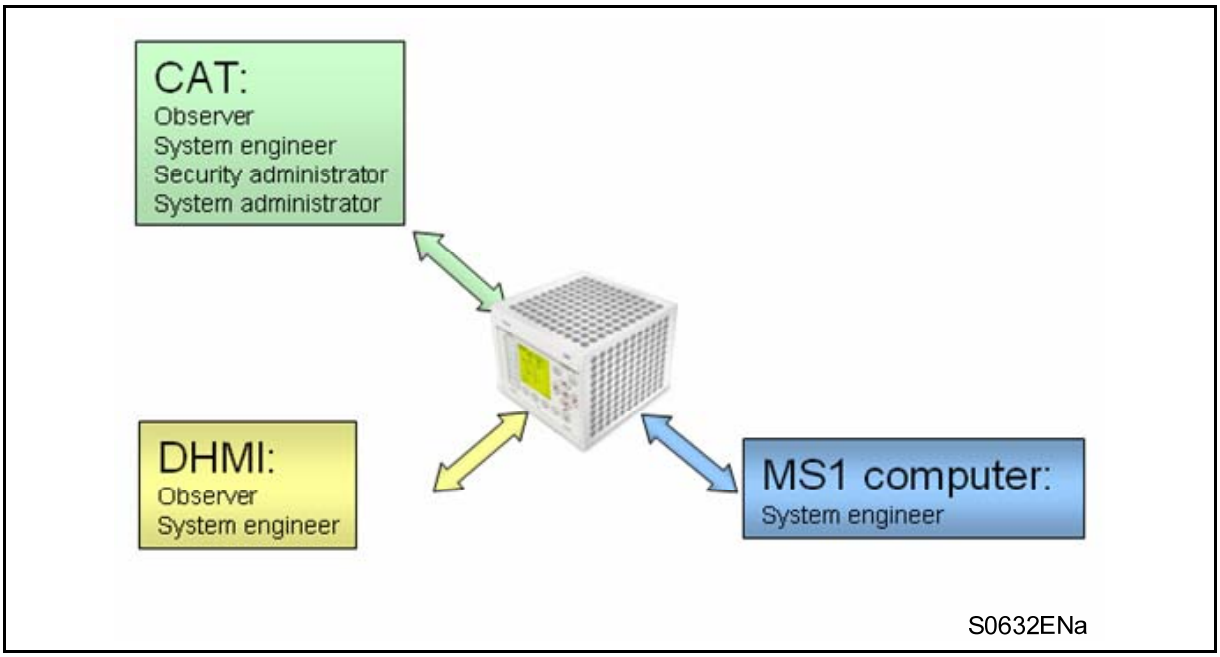
The privileges cumulate starting from Observer up to System administrator.

Privileges	Eligibility
Change the software content	System administrator
Enable/disable communication ports	
Change a sub-system operating mode	
Download database	System administrator + System engineer
Change settings, place commands	
View data	System administrator + System engineer + Observer

A fourth profile is the Security administrator, who is only in charge of the security policy. He/she has exclusive capacity to change passwords.

No other profile than the four mentioned ones can be created.

The authentication server hosted in C264 has three clients (MS1 is MiCOM S1 for short):



For the same login, the password is the same on all computers. Two profiles sharing the same credentials (login + password) differ in their privileges as the applications are different.

It is NOT possible to open several sessions at a time. In other words, if a user is connected to a C264 using one tool, another user can NOT be connected to this C264 using another tool even with another account.

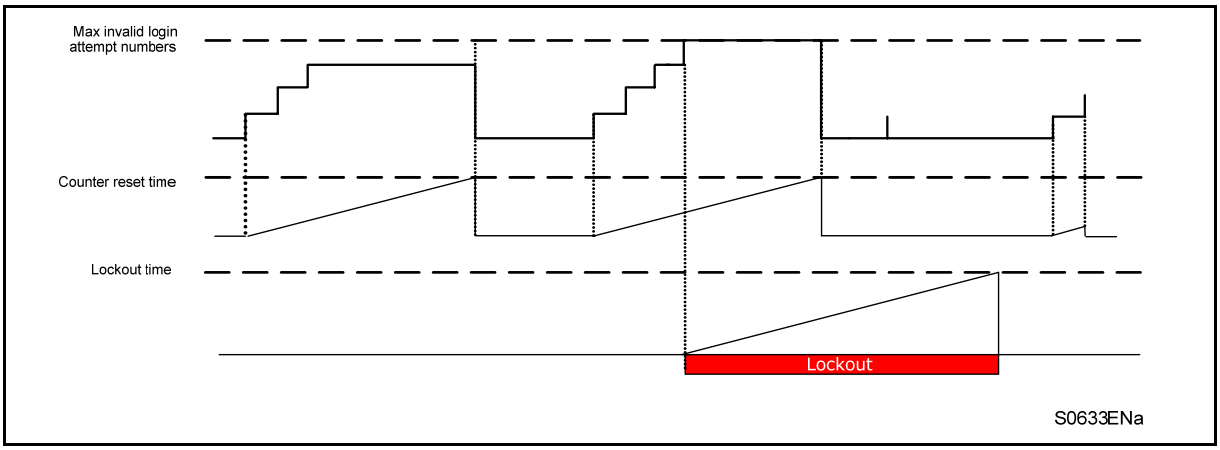
5.4.3 Profile lockout

The lockout is the automatic blocking of a session; viewing of the current screen is still possible. Any new login attempt, even with a correct password, is rejected.

The Security administrator defines the profile lockout policy; if no lockout is defined for a profile, the sessions last as long as the user logs off on his/her own.

Several consecutive failed login attempts result in temporary lockout of login. CAT counts the number of consecutive login failures:

1. The first invalid login sets this counter to 1 and starts a timer.
2. Further invalid writes (for the same profile) increment the counter; at timer expiration, or if the correct password is entered, the counter is reset to 0.
3. Once the counter value reaches the configured maximum, the password entry is locked out. A blocking timer is started and any attempt to enter the password result in an error response, irrespective of whether it is a correct password or not. This does not restart the blocking timer. Once the blocking timer has expired, the password entry is unblocked.



In event of reboot, the counters are reset.

The Security administrator is entitled to unlock a profile before the lockout duration expires.

C264 DHMI: any attempt to write to the password entry whilst it is blocked results in a configurable blocking message being shown for 2 seconds such as **NOT ACCEPTED, ENTRY IS BLOCKED**. This is true as long as the time has not elapsed.

5.4.4 Default password

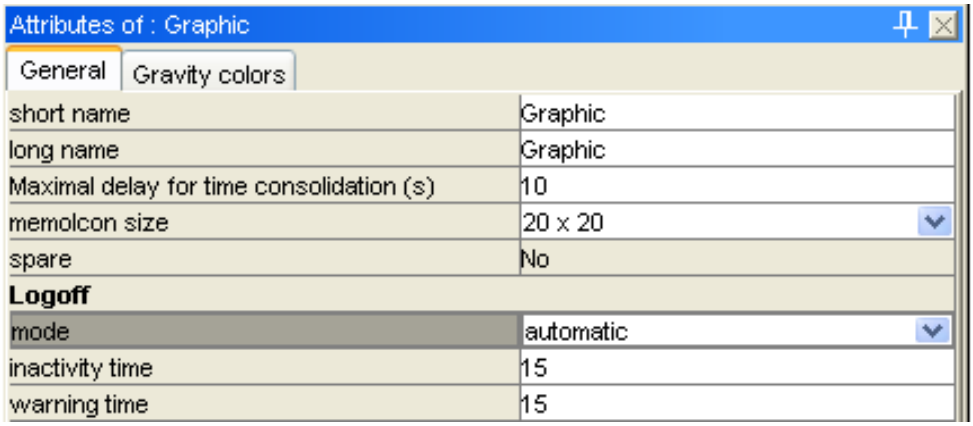
- SMT : network name of machine
- C264 : AAAAAAAA (8 x A)
- CAT : AAAAAAAA (8 x A)
- Switch manager: AAAAAAAA (8 x A)

5.5 Log off after x minutes of inactivity

Automatic logoff after a set time is an option.

- For CAT or MiCOM S1 session, the timeout is set using CAT.
- For DHMI session, the timeout is configured using SCE,
  - Two time values are set to rule the automatic disconnection of graphics:
    - Inactivity time: inactivity time before auto logoff occurs (in minutes)
    - Warning time: visual notification before auto logoff (in seconds)

As long as the inactivity time has not elapsed, you can run another command. This delay is re-armed at each button press. The panel saver is configurable.



- For SMT session, the timeout is set by default to 10 minutes and can be configured for SMT Kernel via "set password HMI".

5.6 Device hardening and EWF

The Enhanced Write Filter (or EWF) is a component of **Windows XP Embedded** which filters writes to another medium instead of being physically written to the volume itself. EWF allows the writes to be discarded or committed to the physical volume.

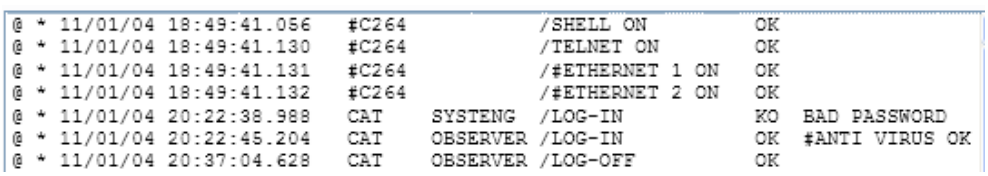
Best practices are indicated by **Schneider-Electric Platform Microsoft Windows XP hardening** recommendations. These recommendations give a brief description of standards tools provided with Windows OS (XP sp3) to help to secure a PC through physical and software hardening, and with account policies enforcement.

5.7 Security logs

The applications record actions related to cyber security in a circular buffer (the size of the file depends on the sub-system capabilities). It includes the following information:

- Date and time: year, month, day, hour, minute, second and millisecond
- User level that performed the changes
- Actions:
  - Antivirus efficiency
  - Login: successful or not or attempt
  - Manual/Automatic logoff
  - Port disabled
  - Firmware change: resulting in a firmware change
  - Password level change
  - Security log viewing/downloading

Example:



```
@ * 11/01/04 18:49:41.056   #C264           /SHELL ON          OK
@ * 11/01/04 18:49:41.130   #C264           /TELNET ON         OK
@ * 11/01/04 18:49:41.131   #C264           /#ETHERNET 1 ON    OK
@ * 11/01/04 18:49:41.132   #C264           /#ETHERNET 2 ON    OK
@ * 11/01/04 20:22:38.988   CAT    SYSTENG   /LOG-IN            KO  BAD PASSWORD
@ * 11/01/04 20:22:45.204   CAT    OBSERVER  /LOG-IN            OK  #ANTI VIRUS OK
@ * 11/01/04 20:37:04.628   CAT    OBSERVER  /LOG-OFF           OK
```

5.8 Antivirus

The Windows-based PCs are vulnerable to viruses.

At application launch, the PC does a check for an antivirus presence. In case of absence, it is up to the user to move on or not as stated:

CAT Antivirus Warning
Antivirus check failed :No antivirus found
You can either close CAT by clicking on button 'Cancel' or continue working with CAT by clicking on button 'Continue'. If you choose to continue, you must be aware and understand the risk
Continue
Cancel

At application launch, the PC does a check for the virus signatures list date:

- if the list is up-to-date, the application moves on
- Otherwise, the user is advised to update it.

The check result is recorded in the security log.

A PC hosting NON time-critical applications can be permanently scanned by an antivirus.

The PCs hosting time-critical applications such as PACiS OI and GTW can NOT be permanently scanned; therefore the user must closely monitor any data intake through drives.

A PC Guard serves as a check-up hub to any movable media before data transfer.The PACIS CYBER tool for software updating and PC scanning is supported.

Please refer to **PACiS Cyber Tools** recommendations in order to**:**

- Install and update antivirus on PC Guard,
- Check media on PC Guard.

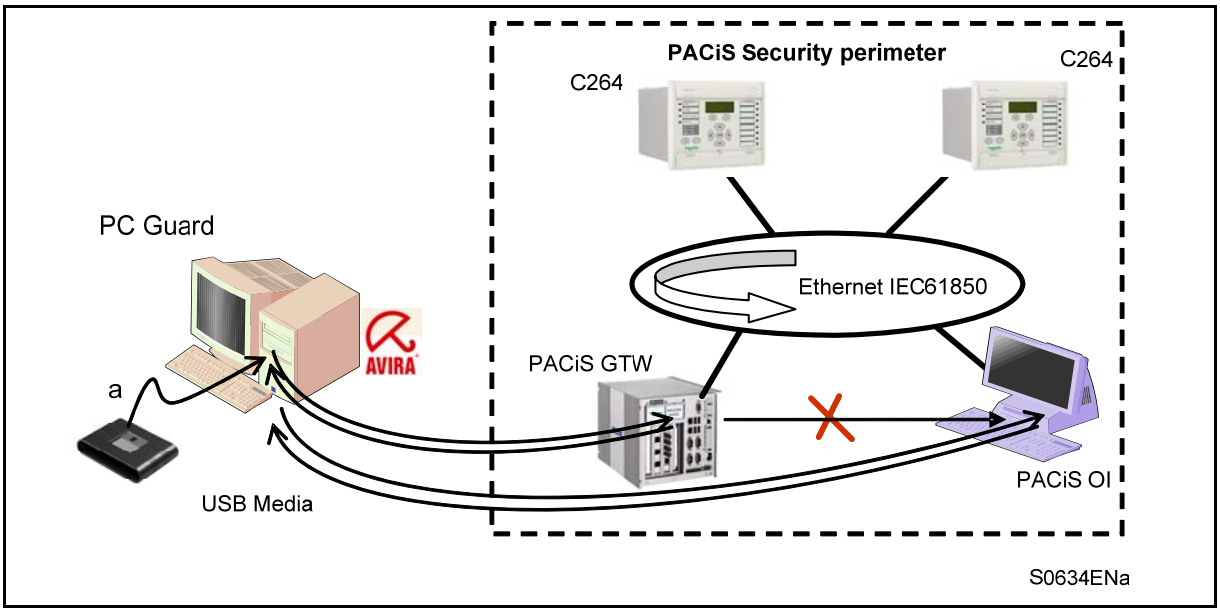


FIGURE 1: THE WHOLE PROCESS AT A GLANCE

6. APPENDIX

6.1 Port reservation

PACiS Applications ports reservation

Application	Function	USED Port IP
SMT	RMI Broadcast	3000 10000
AGENCY		102 103
GATEWAY	DNP3 T104 MODBUS TCP/IP	20000 2404 502
CAT	Security layer used by CAT	9999, 9997
C264	T104 DNP3 Telnet IEC 61850 RPC for tunneling Web server Security layer used by C264	2404 20000 23 102 111 80 9999, 9997
MiCOM S1	Security layer used by MS1	9999, 9997

BLANK PAGE

Customer Care Centre

http://www.schneider-electric.com/CCC

Schneider Electric

35 rue Joseph Monier
92506 Rueil-Malmaison
FRANCE

Phone: +33 (0) 1 41 29 70 00
Fax: +33 (0) 1 41 29 71 00

www.schneider-electric.com

Publication: PACiS/EN TG/C80

Publishing: Schneider Electric
10/2011

© 2011 Schneider Electric. All rights reserved.